

**DIGITAL IMAGE WATERMARKING USING
MULTIWAVELET TRANSFORM**

Prayoth Kumsawat

**A Thesis Submitted in Fulfillment of the Requirements for the
Degree of Doctor of Philosophy in Electrical Engineering**

Suranaree University of Technology

Academic Year 2005

ISBN 974-533-537-1

การทำภาพพิมพ์ลายน้ำดิจิทัลโดยใช้การแปลงมัลติเวฟเล็ท

ร.อ.ประโยชน์ คำสวัสดิ์

วิทยานิพนธ์นี้สำหรับการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรดุษฎีบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า

มหาวิทยาลัยเทคโนโลยีสุรนารี

ปีการศึกษา 2548

ISBN 974-533-537-1

DIGITAL IMAGE WATERMARKING USING MULTIWAVELET TRANSFORM

Suranaree University of Technology has approved this thesis submitted in fulfillment of the requirements for the Degree of Doctor of Philosophy.

Thesis Examining Committee



(Assoc. Prof. Dr. Sarawut Sujitjorn)

Chairperson



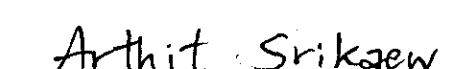
(Asst. Prof. Dr. Kitti Attakitmongkol)

Member (Thesis Advisor)



(Asst. Prof. Dr. Warakorn Charoensuk)

Member



(Asst. Prof. Dr. Arthit Srikaew)

Member



(Dr. Thanatchai Kulworawanichpong)

Member



(Assoc. Prof. Dr. Vorapot Khompis)



(Assoc. Prof. Dr. Saowanee Rattanaphani)

Vice Rector for Academic Affairs

Dean of Institute of Engineering

ประโยชน์ คำสวัสดิ์ : การทำภาพพิมพ์ลายน้ำดิจิทัลโดยใช้การแปลงมัลติเวฟเล็ด

(DIGITAL IMAGE WATERMARKING USING MULTI-WAVELET



TRANSFORM) อาจารย์ที่ปรึกษา : ผู้ช่วยศาสตราจารย์ ดร.กิตติ อัครกิจมงคล, 196 หน้า.

ISBN 974-533-537-1

งานวิจัยวิทยานิพนธ์นี้นำเสนอการวิจัยและพัฒนาการทำภาพพิมพ์ลายน้ำดิจิทัลโดยใช้การแปลงมัลติเวฟเล็ด โดยได้แบ่งหัวข้อในการวิจัยออกเป็นสองส่วน ส่วนแรกเป็นการวิจัยในขั้นพื้นฐาน โดยได้ทำการตรวจวิเคราะห์ผลกระทบของวิธีการแปลงสัญญาณภาพที่มีต่อการทำภาพพิมพ์ลายน้ำดิจิทัลที่ใช้หลักการกระจายแถบความถี่ วิธีการแปลงสัญญาณภาพที่นำเสนอประกอบด้วย การแปลงโคไซน์แบบดิสครีต การแปลงเวฟเล็ดแบบดิสครีตและการแปลงมัลติเวฟเล็ดแบบดิสครีต ผู้วิจัยได้ทำการจำลองการทำงาน โดยศึกษาว่าสัมประสิทธิ์การแปลงของแต่ละวิธีมีผลต่อคุณภาพของภาพเอาต์พุตและความทนทานของสัญญาณลายน้ำอย่างไร นอกจากนี้ผู้วิจัยยังได้ทำการตรวจวิเคราะห์ผลกระทบของวิธีการรวมกลับสัญญาณที่มีมัลติเวฟเล็ดฟิลเตอร์แบงก์เพื่อเลือกวิธีการรวมกลับสัญญาณที่เหมาะสมเพื่อนำไปใช้ในการออกแบบอัลกอริทึมการทำภาพพิมพ์ลายน้ำดิจิทัลที่ใช้การแปลงมัลติเวฟเล็ดต่อไป ส่วนที่สองของงานวิจัยเป็นการออกแบบ โดยได้นำเสนอแนวทางใหม่ในการหาค่าเหมาะที่สุดของระบบการทำภาพพิมพ์ลายน้ำดิจิทัลที่ใช้การแปลงมัลติเวฟเล็ด โดยผู้วิจัยได้ใช้จินเนติกอัลกอริทึมในการหาค่าเหมาะที่สุด โดยทำการค้นหาค่าพารามิเตอร์ในการทำภาพพิมพ์ลายน้ำดิจิทัลประกอบด้วยค่าความแรงแรงของสัญญาณลายน้ำและค่าจุดเริ่มเปลี่ยนในการฝัง และการตรวจจับสัญญาณลายน้ำซึ่งผลที่ได้ทำให้ระบบมีคุณภาพของภาพเอาต์พุตที่ดีและมีความทนทานของสัญญาณลายน้ำดีกว่าระบบเดิม สัญญาณลายน้ำที่ใช้ในวิธีการนี้เป็นลำดับของจำนวนจริงแบบสุ่ม และเพื่อให้อัลกอริทึมที่ทำการออกแบบขึ้นสามารถนำไปประยุกต์ใช้ได้อย่างหลากหลาย ผู้วิจัยได้ทำการคิดค้นและพัฒนาอัลกอริทึมการทำภาพพิมพ์ลายน้ำดิจิทัลขึ้นใหม่ โดยใช้เทคนิคแผนภูมิต้นไม้ของมัลติเวฟเล็ดในการฝังสัญญาณลายน้ำซึ่งเป็นข้อมูลไบนารี เทคนิคดังกล่าวสามารถทำการคัดแยกสัญญาณลายน้ำออกมาได้โดยไม่จำเป็นต้องใช้ภาพต้นฉบับแต่อย่างใด จากการจำลองการทำงานพบว่าสัญญาณลายน้ำที่ฝังไว้ไม่สามารถสังเกตเห็นได้ด้วยตาเปล่าและมีความทนทานต่อการประมวลผลสัญญาณแบบต่างๆ หัวข้อสุดท้ายของการออกแบบได้นำเสนอการเปรียบเทียบประสิทธิภาพของการทำภาพพิมพ์ลายน้ำดิจิทัลในโดเมนของการแปลงมัลติเวฟเล็ด โดยได้นำระบบการทำภาพพิมพ์ลายน้ำดิจิทัลที่ใช้เทคนิคแผนภูมิต้นไม้ของมัลติเวฟเล็ดซึ่งได้ทำการออกแบบไว้ข้างต้นมาทำการเปรียบเทียบประสิทธิภาพกับระบบที่ใช้เทคนิคการเข้ารหัสสัญญาณแบบ Code Division Multiple Access (CDMA) สัญญาณลายน้ำที่ใช้ถูกปรับเปลี่ยนรูปแบบมาเป็นภาพสัญลักษณ์ วิธีการเปรียบเทียบดังกล่าวได้กระทำที่ระดับคุณภาพของสัญญาณ

ภาพเดียวกันโดยใช้ค่า Normalized Correlation และ Bit Error Rate ในการเปรียบเทียบ
ประสิทธิภาพของการทำภาพพิมพ์ถายน้ำดิจิตอล

สาขาวิชา วิศวกรรมไฟฟ้า
ปีการศึกษา 2548

ลายมือชื่อนักศึกษา 
ลายมือชื่ออาจารย์ที่ปรึกษา 

PRAYOTH KUMSAWAT : DIGITAL IMAGE WATERMARKING USING
MULTIWAVELET TRANSFORM. THESIS ADVISOR : ASST. PROF. KITTI
ATTAKITMONGCOL, Ph.D. 196 PP. ISBN 974-533-537-1

WATERMARKING/MULTIWAVELET/MULTIWAVELET TREE/
GENETIC ALGORITHM

This doctoral thesis presents the research and development of multiwavelet-based image watermarking algorithms by classifying the research topics into two parts. In the fundamental part, we investigate the effects of different types of transformation methods in the spread spectrum image watermarking algorithm including discrete cosine transform, discrete wavelet transform, and discrete multiwavelet transform. The efficacies of these transformation methods are discussed by evaluating watermarked image quality and robustness of the watermarks. We also investigate the effects of the recombining processes for multiwavelet filter banks to image watermarking. The performance of private and public watermarking schemes with different methods of the recombining processes is measured by the robustness of the watermark. The simulation results can clarify the effects of the recombining processes in terms of robustness of the watermark and we can select the suitable recombining method for the further design of robust image watermarking algorithm. In the design part, we present a new approach for optimization in multiwavelet-based image watermarking. Performance improvement with respect to existing algorithms is obtained by genetic algorithm optimization. In our optimization process, we search for parameters which consist of threshold values and embedding strength to improve the visual quality of

watermarked images and the robustness of the watermark. The watermark is a sequence of randomly generated real numbers which can only be detected by employing the detection algorithm. In order to use an image watermarking algorithm to a variety of applications, it is required that the watermark be binary and be extractable. Consequently, we have developed a novel robust image watermarking algorithm based on the multiwavelet-tree. The embedding information is binary data and it cannot only be detectable but also extractable. Moreover, this technique does not require the original image in the watermark extraction. The experimental results show that the proposed algorithm yields a watermark which is invisible to human eyes and robust to various image manipulations. The final topic of the design part presents the performance comparison of image watermarking schemes in the multiwavelet transform domain. The first watermarking scheme is based on the concept of multiwavelet-tree and the second is based on the code division multiple access (CDMA) technique. In this comparison, the embedding information is a binary logo image. The normalized correlation and bit error rate are used to evaluate the robustness of the watermark. The evaluation process of robustness is performed on the watermarked images from both techniques under the same image quality.

School of Electrical Engineering

Academic Year 2005

Student's Signature Bayuth Kumsawat

Advisor's Signature Kitt

TABLE OF CONTENTS

	PAGE
ABSTRACT (THAI).....	I
ABSTRACT (ENGLISH).....	III
ACKNOWLEDGMENTS.....	V
TABLE OF CONTENTS.....	VI
LIST OF TABLES.....	XV
LIST OF FIGURES.....	XVII
LIST OF SYMBOLS AND ABBREVIATIONS.....	XXVIII
CHAPTER	
I INTRODUCTION.....	1
1.1 Problems and rationale.....	1
1.2 Research objectives.....	3
1.3 Benefits of the study.....	3
1.4 Thesis organization.....	4
II LITERATURE REVIEW.....	6
2.1 Introduction.....	6
2.2 Digital image watermarking classifications.....	7
2.2.1 Classification by processing domain.....	7
2.2.1.1 Spatial domain watermarking.....	7
2.2.1.2 Transform domain watermarking.....	7

TABLE OF CONTENTS (Continued)

	PAGE
2.2.2 Classification by the necessary data for detection.....	8
2.2.2.1 Private watermarking.....	8
2.2.2.2 Semi-private watermarking.....	8
2.2.2.3 Public watermarking.....	8
2.3 Digital image watermarking in transform domains.....	9
2.3.1 Discrete cosine transform-based image watermarking.....	9
2.3.2 Wavelet-based image watermarking.....	10
2.3.3 Multiwavelet-based image watermarking.....	12
2.4 Artificial intelligent-based image watermarking.....	13
2.5 Chapter Summary.....	14
III THEORETICAL BACKGROUNDS.....	15
3.1 Introduction.....	15
3.2 Multiwavelet.....	16
3.2.1 Multiwavelet transform.....	16
3.2.2 The recombining processes for the multiwavelet filter bank.....	22
3.3 Digital watermarking.....	25
3.3.1 Digital watermarking framework.....	25
3.3.2 Requirements of digital watermarking.....	31

TABLE OF CONTENTS (Continued)

	PAGE
3.3.2.1 Perceptual invisibility.....	31
3.3.2.2 Robustness.....	31
3.3.2.3 Data capacity.....	32
3.3.2.4 Unambiguous.....	32
3.3.3 Performance measures.....	32
3.3.3.1 Peak signal to noise ratio.....	33
3.3.3.2 Universal quality index.....	33
3.3.3.3 Correlation coefficient.....	34
3.3.3.4 Bit error rate.....	34
3.3.3.5 Computational complexity.....	35
3.3.4 Applications of digital watermarking.....	35
3.3.4.1 Copyright protection.....	35
3.3.4.2 Fingerprinting.....	36
3.3.4.3 Copy protection.....	36
3.3.4.4 Broadcast monitoring.....	36
3.3.4.5 Data authentication.....	37
3.4 Chapter Summary	37
IV EFFECTS OF TRANSFORMATION METHODS	
ON IMAGE WATERMARKING.....	38
4.1 Introduction.....	38

TABLE OF CONTENTS (Continued)

	PAGE
4.1.1 Previous works.....	39
4.2 Evaluation method.....	39
4.2.1 Spread spectrum image watermarking.....	40
4.2.1.1 Watermark embedding algorithm.....	40
4.2.1.2 Watermark extracting algorithm.....	41
4.3 Results and discussions.....	44
4.3.1 Imperceptibility.....	44
4.3.2 Robustness.....	49
4.4 Chapter Summary	54
V EFFECTS OF THE RECOMBINING PROCESSES FOR THE MULTIWAVELET FILTER BANK ON IMAGE WATERMARKING.....	55
5.1 Introduction.....	55
5.1.1 Previous works.....	56
5.2 Evaluation method.....	57
5.2.1 The recombining processes for the multiwavelet filter bank.....	57
5.2.2 Public watermarking scheme.....	60
5.2.2.1 Watermark embedding algorithm.....	60
5.2.2.2 Watermark detection algorithm.....	61

TABLE OF CONTENTS (Continued)

	PAGE
5.3 Results and discussions.....	64
5.3.1 Results of the private watermarking scheme.....	64
5.3.2 Results of the public watermarking scheme.....	68
5.4 Chapter Summary	71
VI PERFORMANCE IMPROVEMENT OF IMAGE	
WATERMARKING SCHEME USING GENETIC	
ALGORITHMS.....	72
6.1 Introduction.....	72
6.1.1 Previous work.....	73
6.1.2 Contributions.....	74
6.2 Proposed technique.....	75
6.2.1 Multiwavelet-based image watermarking	
algorithm.....	75
6.2.2 Improving watermarking performance by GA.....	75
6.3 Results and discussions.....	79
6.3.1 Results of performance improvement by GA.....	79
6.3.2 Invisibility test results.....	87
6.3.3 Robustness test results.....	90
6.4 Chapter Summary	96

TABLE OF CONTENTS (Continued)

	PAGE
VII A NOVEL ROBUST IMAGE WATERMARKING	
TECHNIQUE BASED ON MULTIWAVELET	
TRANSFORM.....	97
7.1 Introduction.....	97
7.1.1 Previous work.....	98
7.1.2 Contributions.....	99
7.2 Multiwavelet-tree.....	99
7.3 Proposed technique.....	102
7.3.1 Watermark embedding algorithm.....	102
7.3.2 Watermark extracting algorithm.....	106
7.3.3 Watermark detection analysis.....	107
7.4 Results and discussions.....	111
7.4.1 Invisibility test results.....	112
7.4.2 Robustness test results.....	113
7.5 Chapter Summary.....	120
VIII COMPARATIVE PERFORMANCE OF MULTIWAVELET-	
BASED IMAGE WATERMARKING SCHEMES.....	121
8.1 Introduction.....	121
8.1.1 Previous works.....	121

TABLE OF CONTENTS (Continued)

	PAGE
8.2 Multiwavelet-based image watermarking scheme.....	123
8.2.1 Multiwavelet-tree watermarking technique.....	123
8.2.1.1 Watermark embedding algorithm.....	123
8.2.1.2 Watermark extracting algorithm.....	124
8.2.2 CDMA watermarking technique.....	124
8.2.2.1 Watermark embedding algorithm.....	125
8.2.2.2 Watermark extracting algorithm.....	126
8.3 Results and discussions.....	129
8.4 Chapter Summary	141
IX MULTIWAVELET TOOLBOX AND MULTIWAVELET	
TREE IMAGE WATERMARKING PROGRAM.....	142
9.1 Introduction.....	142
9.2 Multiwavelet toolbox for MATLAB.....	143
9.2.1 Hardware and software requirements	143
9.2.2 Toolbox structure.....	143
9.2.3 Limitation of toolbox.....	144
9.2.4 List of functions in toolbox.....	145
9.2.4.1 Functions for one-dimensional signal	145
9.2.4.2 Functions for two-dimensional signal	146
9.2.5 M-file examples.....	148

TABLE OF CONTENTS (Continued)

	PAGE
9.2.6 Execution time testing.....	151
9.3 Multiwavelet tree image watermarking program.....	152
9.3.1 Basic requirements.....	152
9.3.2 Program structure.....	152
9.3.2.1 Window appearance of the GUI.....	153
9.3.2.2 Watermark embedding routine.....	154
9.3.2.3 Watermark extracting routine.....	154
9.3.3 Example of program usage.....	156
9.3.3.1 Watermark embedding procedures.....	156
9.3.3.2 Watermark extracting procedures.....	157
9.4 Chapter Summary.....	159
X CONCLUSIONS AND FUTURE STUDIES.....	160
10.1 Conclusions.....	160
10.1.1 The effects of transformation methods on image watermarking.....	160
10.1.2 The effects of the recombining processes for the multiwavelet filter bank on image watermarking.....	161
10.1.3 Performance improvement of image watermarking scheme using genetic algorithms.....	161

TABLE OF CONTENTS (Continued)

	PAGE
10.1.4 A novel robust image watermarking technique based on multiwavelet transform.....	162
10.1.5 Comparative performance of multiwavelet-based image watermarking schemes.....	162
10.2 Future studies.....	163
REFERENCES.....	165
APPENDICES	
APPENDIX A. MULTIREOLUTION ANALYSIS.....	174
APPENDIX B. PUBLICATIONS RELATED TO THE PhD RESEARCH.....	178
APPENDIX C. MULTITREE WATERMARK.....	182
APPENDIX D. WAVELET TREE WATERMARKING ALGORITHM.....	193
BIOGRAPHY.....	196

LIST OF TABLES

TABLE	PAGE
4.1 PSNR of watermarked images using 5 test images.....	48
4.2 Embedding strengths of watermark signal for the test images.....	50
6.1 Parameters α , T_1 and T_2 from GA search of the Lena image.....	85
6.2 Parameters α , T_1 and T_2 from GA search of the Baboon image.....	85
6.3 Parameters α , T_1 and T_2 from GA search of the Gold Hill image.....	86
6.4 Parameters α , T_1 and T_2 from GA search of the Pepper image.....	86
6.5 Comparison of PSNR between Dugads, DugadDMT1 and GADugadDMT1 methods.....	89
6.6 Comparison of UQI between Dugads, DugadDMT1 and GADugadDMT1 methods.....	90
7.1 False alarm probability for different thresholds.....	116
7.2 Normalized correlation using JPEG compression.....	118
7.3 Normalized correlation using SPIHT compression.....	118
7.4 Normalized correlation using image processing attacks.....	119
8.1 False alarm probability for different thresholds.....	132
8.2 Extracted logos from watermarked image after JPEG compression with various quality factors.....	135

LIST OF TABLES (Continued)

TABLE	PAGE
8.3 The normalized correlation coefficient and bit error rate from two different multiwavelet-based image watermarking techniques using Lena image.....	139
8.4 The normalized correlation coefficient and bit error rate from two different multiwavelet-based image watermarking techniques using Baboon image.....	140
9.1 The execution time for multiwavelet decomposition and reconstruction.....	151
C.1 Images from digital camera (all images are in JPEG file format).....	184
C.2 Images from electron microscope.....	184
C.3 The results of invisibility and robustness test using images from digital camera.....	191
C.4 The results of invisibility and robustness test using images from electron microscope.....	192

LIST OF FIGURES

FIGURE	PAGE
3.1 DGHM scaling functions (a) $\phi_1(t)$ (b) $\phi_2(t)$	19
3.2 DGHM wavelet functions (a) $\psi_1(t)$ (b) $\psi_2(t)$	20
3.3 Multiwavelet filter bank.....	21
3.4 Image subbands of single-level decomposition using (a) method 1 and (b) method 2.....	24
3.5 Three-level decomposition of the Lena image using the DGHM multiwavelet (with prefiltering) and the recombining (a) method 1 and (b) method 2.....	24
3.6 Standard model of communication system.....	27
3.7 The model of watermarking systems with (a) informed detector and (b) blind detector.....	28
4.1 Watermark embedding process by using DCT.....	41
4.2 Watermark extracting process by using DCT.....	43
4.3 (a) Original “Lena” image and transformed coefficients of the (b) DCT, (c) DWT and (d) DMT.....	46
4.4 (a) Watermarked “Lena” image using DCT method and (b) absolute difference between the original image and the watermarked image, magnified by a factor 8.....	47

LIST OF FIGURES (Continued)

FIGURE	PAGE
4.5 (a) Watermarked “Lena” image using DWT method and (b) absolute difference between the original image and the watermarked image, magnified by a factor 8.....	47
4.6 (a) Watermarked “Lena” image using DMT method and (b) absolute difference between the original image and the watermarked image, magnified by a factor 8.....	48
4.7 PSNR of (a) Lena and (b) Baboon watermarked images with different watermark strengths.....	49
4.8 Detector response of 1,000 watermarks including extracted watermark of (a) Lena image and (b) Baboon image using DCT under 10 % JPEG quality.....	51
4.9 Similarities of watermarks under JPEG compression (a) Lena and (b) Baboon.....	52
4.10 Similarities of watermarks under lowpass filtering (a) Lena and (b) Baboon.....	52
4.11 Similarities of watermarks under Wiener filtering (a) Lena and (b) Baboon.....	53

LIST OF FIGURES (Continued)

FIGURE	PAGE
4.12 Similarities of watermarks under Gaussian noise addition (a) Lena and (b) Baboon.....	53
5.1 Image subbands of single-level decomposition using (a) method 1 and (b) method 2.....	59
5.2 Three-level decomposition of the Lena image using the DGHM multiwavelet (with prefiltering) and the recombining (a) method 1 and (b) method 2.....	60
5.3 Watermark embedding process.....	63
5.4 Watermark detection process.....	63
5.5 Similarity measurements of (a) Lena and (b) Baboon images under JPEG compression attack.....	66
5.6 Similarities of watermarks under lowpass filtering using (a) Lena and (b) Baboon images.....	66
5.7 Similarities of watermarks under Wiener filtering using (a) Lena and (b) Baboon images.....	67
5.8 Similarities of watermarks under Gaussian noise addition using (a) Lena and (b) Baboon images.....	67

LIST OF FIGURES (Continued)

FIGURE	PAGE
5.9 Correlation output of (a) Lena and (b) Baboon images under JPEG compression attack.....	69
5.10 Correlation output of watermarks under lowpass filtering using (a) Lena and (b) Baboon images.....	70
5.11 Correlation output of watermarks under Wiener filtering using (a) Lena and (b) Baboon images.....	70
5.12 Correlation output of watermarks under Gaussian noise addition using (a) Lena and (b) Baboon images.....	71
6.1 Optimization diagram for digital image watermarking using GA.....	78
6.2 The results of ALPHA (α), T_1 , and T_2 for probability of crossover varying from 0.1 to 1.0.....	80
6.3 The results of ALPHA (α), T_1 , and T_2 for probability of mutation varying from 0.001 to 0.015.....	81
6.4 The results of ALPHA (α), T_1 , and T_2 by varying the number of chromosomes from 10 to 100.....	81
6.5 UQI , DIF and W from optimization process of (a) LH_2 and (b) HL_2 subbands for Lena image.....	82
6.6 UQI , DIF and W from optimization process of (a) HH_2 and (b) LH_3 subbands for Lena image.....	82

LIST OF FIGURES (Continued)

FIGURE	PAGE
6.7 UQI , DIF and W from optimization process of (a) HL_3 and (b) HH_3 subbands for Lena image.....	83
6.8 UQI , DIF and W from optimization process of (a) LH_2 and (b) HL_2 subbands for Baboon image.....	83
6.9 UQI , DIF and W from optimization process of (a) HH_2 and (b) LH_3 subband for Baboon image.....	84
6.10 UQI , DIF and W from optimization process of (a) HL_3 and (b) HH_3 subband for Baboon image.....	84
6.11 (a) Original Lena image and (b) watermarked image with PSNR 46.07 dB.....	87
6.12 (a) Original Baboon image and (b) watermarked image with PSNR 41.87 dB.....	88
6.13 (a) Original Gold Hill image and (b) watermarked image with PSNR 45.66 dB.....	88
6.14 (a) Original Pepper image and (b) watermarked image with PSNR 44.48 dB.....	89

LIST OF FIGURES (Continued)

FIGURE	PAGE
6.15 Different type of attacks to watermarked image (a) JPEG compression (quality factor 10%), (b) lowpass filtering (9×9), (c) Wiener filtering (9×9), (d) Gaussian noise addition (variance 500), (e) cropping 50% of its surrounding and (f) image rotation (1.0° clockwise).....	91
6.16 JPEG compression attack (quality factor 10%). (a) Detector response of 6 subbands. (b) Detector response of the extracted watermark of subband LH_2 when 1,000 watermarks were tested.....	92
6.17 Correlation output using JPEG compression with various qualities of (a) Lena image and (b) Baboon image.....	92
6.18 Correlation output using lowpass filtering with various sizes of window filters of (a) Lena image and (b) Baboon image.....	94
6.19 Correlation output using Wiener filtering with various sizes of window filters of (a) Lena image and (b) Baboon image.....	94
6.20 Correlation output using Gaussian noise addition with various noise variances of (a) Lena image and (b) Baboon image.....	95
6.21 Correlation output using cropping with various cropping areas of (a) Lena image and (b) Baboon image.....	95
6.22 Correlation output using rotation with various rotation angles of (a) Lena image and (b) Baboon image.....	96

LIST OF FIGURES (Continued)

FIGURE	PAGE
7.1 (a) Four-level multiwavelet decomposition of image having size of 512 × 512 pixels and (b) the parent-child dependencies of multiwavelet-tree.....	100
7.2 (a) A group of multiwavelet coefficients in each tree and (b) an example of triple tree.....	101
7.3 JPEG quantization matrix.....	104
7.4 Watermark embedding process.....	104
7.5 Flow chart of the proposed watermark embedding algorithm.....	105
7.6 Flow chart of the proposed watermark extracting algorithm.....	108
7.7 Watermark extracting process.....	109
7.8 (a) Original “Lena” image and (b) watermarked image from the proposed method.....	112
7.9 (a) Original “Baboon” image and (b) watermarked image from the proposed method.....	113
7.10 Plots of (a) Normalized correlation coefficient and (b) BER versus different compression ratio of JPEG compression using Lena and Baboon image.....	116

LIST OF FIGURES (Continued)

FIGURE	PAGE
7.11 Plots of (a) Normalized correlation coefficient and (b) BER versus different compression ratio of JPEG2000 compression using Lena and Baboon image.....	117
7.12 Plots of (a) Normalized correlation coefficient and (b) BER versus different cropping ratio of cropping attack using Lena and Baboon image.....	117
8.1 Watermark embedding process.....	125
8.2 Watermark extraction process.....	125
8.3 Flow chart of the CDMA watermark embedding algorithm.....	127
8.4 Flow chart of the CDMA watermark extracting algorithm.....	128
8.5 (a) Original watermark and (b) permuted watermark.....	130
8.6 (a) Original “Lena” image and (b) watermarked image from DMT-Tree.....	130
8.7 (a) Original “Baboon” image and (b) watermarked image from DMT-Tree.....	131
8.8 (a) Original “Lena” image and (b) watermarked image from DMT-CDMA.....	131
8.9 (a) Watermarked “Baboon” image from DMT-Tree and (b) watermarked image from DMT-CDMA.....	132

LIST OF FIGURES (Continued)

FIGURE	PAGE
8.10 Plots of (a) Normalized correlation coefficient and (b) BER versus different JPEG quality factors of JPEG compression using Lena image.....	136
8.11 Plots of (a) Normalized correlation coefficient and (b) BER versus different JPEG quality factors of JPEG compression using Baboon image.....	136
8.12 Plots of (a) Normalized correlation coefficient and (b) BER versus different bit rates of JPEG2000 compression using Lena image.....	137
8.13 Plots of (a) Normalized correlation coefficient and (b) BER versus different bit rates of JPEG2000 compression using Baboon image.....	137
8.14 Plots of (a) Normalized correlation coefficient and (b) BER versus different filter sizes of lowpass filtering using Lena image.....	138

LIST OF FIGURES (Continued)

FIGURE	PAGE
8.15 Plots of (a) Normalized correlation coefficient and (b) BER versus different filter sizes of lowpass filtering using Baboon image.....	138
9.1 Block diagrams of multiwavelet decomposition.....	144
9.2 Block diagrams of multiwavelet reconstruction.....	144
9.3 Prefiltered image.....	149
9.4 The result of one-level decomposition.....	150
9.5 Reconstructed image.....	150
9.6 Screenshot of watermarking program.....	153
9.7 Flow chart for watermark embedding routine.....	155
9.8 Flow chart for watermark extracting routine.....	156
9.9 Watermark embedding procedure.....	157
9.10 Watermarked image.....	158
9.11 Watermark extracting procedure.....	158
9.12 Extracted watermark.....	159
9.13 Warning message if the suspected image does not contain watermark.....	159
A.1 Space expansion of V_j and W_j	176
C.1 Screenshot of MultiTree Watermark program.....	183
C.2 Original images and watermarked images.....	185

LIST OF FIGURES (Continued)

FIGURE	PAGE
C.3 Original images and watermarked images.....	186
C.4 Original images and watermarked images.....	187
C.5 Original images and watermarked images.....	188
C.6 Original images and watermarked images.....	189
C.7 Original images and watermarked images.....	190

LIST OF SYMBOLS AND ABBREVIATIONS

BER	=	Bit Error Rate
BPN	=	Back Propagation Neural network
c	=	Scalar sequence
c_1	=	Lowpass component of multiwavelet transform coefficients
CDMA	=	Code Division Multiple Access
CPTWG	=	Copy Protection Technical Working Group
d_1	=	Highpass component of multiwavelet transform coefficients
DC	=	Direct Current
DCT	=	Discrete Cosine Transform
DFT	=	Discrete Fourier Transform
DGHM	=	Donovan, Geronimo, Hardin and Massopust
DIF	=	The different between correlation z and Threshold S
DMT	=	Discrete Multiwavelet Transform
DRM	=	Digital Rights Management
DVD	=	Digital Versatile Discs
DWT	=	Discrete Wavelet Transform
D_r	=	The operator which partitions a scalar sequence into a sequence grouped in vectors of length r

LIST OF SYMBLOS AND ABBREVIATIONS (Continued)

EE SUT	=	Electrical Engineering, Suranaree University of Technology
f	=	Arbitrary function
GA	=	Genetic Algorithms
$G(z)$	=	The z transform of $g(n)$
$g(n)$	=	Highpass filter coefficients
$H(z)$	=	The z transform of $h(n)$
$H_m(z)$	=	Modulation matrix
HL_1	=	Image subband of High-Low at level one of multiwavelet decomposition
HH_1	=	Image subband of High-High at level one of multiwavelet decomposition
$h(n)$	=	Lowpass filter coefficients
HSV	=	HSV Color space, where H is hue, S is saturation and V is value
HVS	=	Human Visual System
I	=	Identity matrix
i	=	Sequence number
Inverse DCT	=	Inverse Discrete Cosine Transform
ISBN	=	International Standard Book Numbering
ISRC	=	International Standard Recording Code

LIST OF SYMBOLS AND ABBREVIATIONS (Continued)

JPEG	=	Joint Photographic Expert Groups
JND	=	Just Noticeable Differences
j	=	Resolution level
LH_1	=	Image subband of Low-High at level one of multiwavelet decomposition
LL_1	=	Image subband of Low-Low at level one of multiwavelet decomposition
l	=	Number of levels of decomposition
MCR	=	MATLAB TM component runtime
MRA	=	Multiresolution analysis
M	=	Amount of discrete multiwavelet transform coefficient
MPEG	=	Moving Picture Expert Groups
n	=	Amount of data
NVF	=	Noise Visibility Function
N_w	=	Length of watermark sequence
p	=	Approximation order
$P_{fa}(T)$	=	Probability of false alarm
$P_{fr}(T)$	=	Probability of false rejection
$Pr ob\{A B\}$	=	Probability of event A given event B
PSC	=	Perceptually Significant Coefficients
PSNR	=	Peak signal to noise ratio

LIST OF SYMBOLS AND ABBREVIATIONS (Continued)

$P(z)$	=	Prefilter
$Q(z)$	=	Postfilter
R	=	Set of real number
RMSE	=	Root Mean Square Error
RGB	=	RGB Color space, where R is Red, G is Green and B is Blue
r	=	The number of scaling functions
S	=	Decision threshold
SDMI	=	Strategic Digital Music Initiative
T_1	=	Embedding threshold
T_2	=	Detection threshold
Tg_m	=	Group of multiwavelet tree
Tt_n	=	Triple tree
Ttw_i	=	Triple tree that contains watermark information
UQI	=	Universal Quality Index
V_0	=	Vector space
V_i	=	Multiwavelet transform coefficient at sequence i
W	=	Objective function
W_0	=	Multiwavelet space
X	=	Vector sequence
XOR	=	Exclusive OR operator

LIST OF SYMBOLS AND ABBREVIATIONS (Continued)

x_i	=	Watermark sequence number i
X	=	Original watermark
X^*	=	Extract watermark
YUV	=	YUV Color space. This is often referred to as YCbCr.
YIQ	=	YIQ Color space, where Y is luminance, I is hue and Q is saturation.
YCbCr	=	YCbCr Color space, where Y is luminance and CbCr is chrominance
Z	=	Set of the all integers
z	=	Correlation value
α	=	Watermark strength
δ	=	Threshold
δ_{UQI}	=	Weighting factors of UQI
δ_{DIF}	=	Weighting factors of DIF
$\rho(W, \tilde{W})$	=	Normalized correlation between W and \tilde{W}
$\Phi(t)$	=	Scaling function
$\Psi(t)$	=	Wavelet function

CHAPTER I

INTRODUCTION

1.1 Problems and Rationale

With the extensive growth of the Internet and the developments in digital communication and compression technology, digital multimedia contents, such as music, video and image, can be distributed instantaneously across the Internet to end-users. Many media companies sell their digital contents not only through CDs and DVDs but also over the Internet networks. Although digital data has been shown to have many advantages over analog data, one of the potential problems on handling the digital data is that it can be easily altered and duplicated without losing its quality. Thus, without protection and management of digital rights, digital content can be copied and distributed to a large number of recipients, which could cause revenue loss to media companies. Consequently, intellectual property protection is a pressing concern for content owners who are selling and exhibiting digital contents through the Internet.

The first technology that content owners turn to is cryptography. Cryptography is probably the most common method of protecting digital contents (Cox et al., 2002). The content is encrypted prior to delivery and a decryption key is provided only those who have purchased legitimate copies of the digital content. After the receiver has received and decrypted the data, however, the data is identical to the original digital content data and the content has no further protection. It is possible for a pirate to actually purchase the content, use the decryption key to obtain an unprotected copy of

content, and then proceed to distribute illegal copies. Thus, there is a strong need for an alternative technology that can protect digital multimedia content even after it is decrypted. Among the various technologies, digital watermarking technology has the potential to fulfill this need.

Digital watermarking is an emerging technology that embeds hidden copyright information directly into the digital multimedia content in such a way that it always remains present. The embedded information data is referred to as “watermark”. Ideally, there should be no perceptible difference between the watermarked and original data, and the watermark should be easily extractable, reliable and robust against decryption, re-encryption, compression and common signal processing. The information carried by the watermark can be accessed using a detection algorithm with the help of a secret key and can be used to identify the copyright holder and ensure proper payment of royalties.

It is clear that digital watermarking and encryption technologies are complementing each other. Therefore, a reliable digital rights management (DRM) system which is a tool that protects intellectual property during digital content commerce depends on both technologies (Kundur and Karthik, 2004). The main applications of digital watermarking are copyright protection, fingerprinting, copy protection, broadcast monitoring and data authentication. Other applications include indexing of movies, medical safety and data hiding (Langelaar et al., 2000).

This dissertation concentrates on designing watermarking algorithms using multiwavelet transform because it possesses properties which have been shown to be useful in image processing applications; for example, the DGHM multiwavelets simultaneously possess orthogonality, compact support, an approximation order of 2 and symmetry (Geronimo et al., 1994). Therefore, multiwavelet-based watermarking

for copyright protection of digital image will be mainly discussed. However, the general idea presented here is also applicable to other forms of digital multimedia contents.

The rest of the chapter is organized as follows: the research objectives in digital image watermarking are given in Section 1.2. In section 1.3, the benefits of the study are discussed. The outlines of this dissertation can be found in Section 1.4.

1.2 Research Objectives

The objectives of this study are described as follows:

- 1) To develop the multiwavelet transform toolbox for MATLAB. This toolbox can be used in researches and developments of image processing in the future work.
- 2) To design and develop a new image watermarking algorithms for copyright protection applications of digital images using multiwavelet transform.
- 3) To implement the image watermarking prototype program from the watermarking algorithm that has been designed and developed earlier. The prototype will be a graphic user interface (GUI) program.

1.3 Benefits of the Study

The benefits of the study are presented as follows:

- 1) Obtain the multiwavelet transform toolbox for MATLAB. This toolbox will be used in the signal and image processing research group, School of Electrical engineering, Suranaree University of Technology for the future research on image processing.

- 2) Obtain a new image watermarking algorithm based on multiwavelet transform.
- 3) Obtain the image watermarking prototype program for copyright protection application.
- 4) Obtain the international conference proceedings and journal papers about the image watermarking algorithms that have been developed in this research work.
- 5) Initiate research study on multiwavelet-based image watermarking algorithm since there are a few watermarking research based on discrete multiwavelet transform.

1.4 Thesis Organization

This dissertation is organized as follows. In the next chapter, Chapter 2, we present several types of digital image watermarking techniques found in the literatures from text books and academic publications.

Chapter 3 provides theoretical backgrounds of multiwavelet transform and a brief overview of digital watermarking. A general framework for watermark embedding and detection is presented here along with a review of the traditional model of communication system. The basic requirements of digital watermarking were then described in term of perceptual invisibility, robustness and data capacity.

In Chapter 4, we investigate the effects of three different types of transformation methods for image watermarking including discrete cosine transform, discrete wavelet transform and discrete multiwavelet transform.

Then, the effects of the recombining processes for the multiwavelet filter bank are given in Chapter 5. We select two different watermarking schemes and evaluate

their performance in order to choose the best recombining method for our multiwavelet based image watermarking algorithm.

Chapter 6 introduces a new approach for performance improvement in multiwavelet-based image watermarking by using genetic algorithms. Performance comparison between the watermarking algorithms with and without optimization technique is given. The comparison is also made with the result of previous work.

In Chapter 7, we propose a new image watermarking algorithm based on multiwavelet transform which can be portable to a various applications such as copyright protection, fingerprinting and identification. The watermark is a binary watermark which cannot only be detectable but also extractable.

Chapter 8 presents the robustness evaluation of image watermarking techniques in the multiwavelet transform domain. The first watermarking technique is based on the concept of multiwavelet-tree and the second one is based on the code division multiple access (CDMA) technique.

Chapter 9 presents the details of the multiwavelet toolbox which can be used in researches and developments of image processing under the MATLAB environment. This chapter also presents the multiwavelet-tree image watermarking program. This program is implemented by using the graphical user interface environment in MATLAB.

The last chapter, Chapter 10, provides conclusions of the research work and suggestion for future studies.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

Digital image watermarking is one of the most popular approaches considered as a tool for providing the copyright protection of digital images. This technique is based on direct embedding of additional information into the digital images. Theoretically, there should be no perceptible difference between the watermarked image and the original one. In addition, the watermark should be easily extractable, but reliable and robust against image compression or common image processing. By extracting the embedding information, the image ownership can be verified or even an illegal copy source can be traced.

In this chapter, literature surveys of up-to-date digital image watermarking techniques found in several textbooks and research papers are presented. Although a large number of digital image watermarking algorithms have been increasingly released, many of them are private watermarking schemes due to the need for an original image in a detection phase. Consequently, the development of a new public watermarking scheme which satisfies both invisibility and robustness, challenges research aspiration of most researchers in the field of digital image watermarking in the 21st century. This chapter presents literature surveys of digital image watermarking and is organized into five sections. Digital image watermarking classifications are given in Section 2.2. Digital image watermarking in transform domains are given in Section 2.3. The artificial intelligent-based image watermarking techniques are given

in Section 2.4. The summary of this chapter can be found in Section 2.5.

2.2 Digital Image Watermarking Classifications

Digital image watermarking techniques proposed in literature can be classified into many categories depending upon various aspects as follows.

2.2.1 Classification by processing domain

In this aspect, digital image watermarking can be divided into two groups, according to the domain of watermark to be embedded: 1) the spatial domain watermarking and 2) the transform domain watermarking.

2.2.1.1 Spatial domain watermarking

Spatial domain watermarking techniques (Langelaar et al., 2000; Lumini and Maio, 2000) are simple to implement and require less computation cost than the other does. To embed a watermark into a targeted image is obviously straight forward. A pseudorandom noise pattern is generated and then added to the luminance value of its pixels based on a key using linear shift registers or randomly shuffled binary images (Tirkel et al., 1993).

2.2.1.2 Transform domain watermarking

In transform domain techniques, an original image is first transformed to a given domain. A provided watermark signal is also transformed into this domain and therefore superimposed to associated transform coefficients through an underlying embedding algorithm. The watermarked image is finally obtained by applying the inverse transform of the modified transform coefficients. The methods belonging to this group often use discrete cosine transform (DCT), discrete wavelet transforms (DWT) and discrete multiwavelet transform (DMT). Details for each technique will be described in Section 2.3.

It notes that this dissertation focuses on design of robust watermarking systems in the transform domain rather than that in the spatial domain. Thus, spatial domain based techniques will not be discussed any further.

2.2.2 Classification by the necessary data for detection

According to the need for an original image during the watermark detection process, digital image watermarking can be classified into private, semi-private and public watermarking as follows (Lee and Jung, 2001).

2.2.2.1 Private watermarking

Private watermarking requires the original image during the detection process. In general, the original image will be subtracted to a suspected image before performing watermark detection to provide extra robustness of the watermark.

2.2.2.2 Semi-private watermarking

Semi-private or semi-blind watermarking, in contrast, does not require the original image. Instead, some information about an original image is needed for watermark detection, for example, size or some statistical characteristics of the original image.

2.2.2.3 Public watermarking

Public watermarking or blind watermarking requires neither an original image nor an embedded watermark. This watermarking will become important when the original image is not easy to obtain or it is difficult to prove which copy is the original one (Zeng and Liu, 1999). As briefly mentioned, designing a blind watermarking scheme challenges world's watermarking research communities.

2.3 Digital Image Watermarking in Transform Domains

Previous works have shown that the transform domain watermarking is more robust to noise, common image processing and compression than the spatial domain watermarking is (Hartung and Kutter, 1999; Petitcolas et al., 1999; Song and Tan, 2000). Thus, transform domain-based watermarking researches are increasingly conducted by several active teams across the globe. Details of digital image watermarking in the transform domain are reviewed as follows:

2.3.1 Discrete cosine transform-based image watermarking

A discrete cosine transform (DCT) has been the most frequently-used transformation technique in image watermarking. One of the most cited watermarking schemes of this technique is proposed by Cox et al. (1997). The proposed technique is performed by embedding a provided watermark into some of the highest magnitude discrete cosine transform coefficients (perceptually significant coefficients) of an image using a concept of spread spectrum communication. This motivation is based on the fact that any attempt to modify the watermark results in visible degradation of the watermarked image. Since the watermark is cast into the most perceptually significant regions of the original image, it is able to resist common signal processing and geometric distortions. However, this technique is not suitable for many applications because of high complexity of global DCT and the need for the original image during watermark extraction.

Barni et al. (1998) present a public watermarking algorithm based on Cox's algorithm but it does not need the original image for extracting the watermark.

In 1999, block DCT is applied before embedding the watermark and the watermark is embedded only in middle frequency components of the 8×8 DCT blocks.

In the embedding part, low frequency components are left untouched in order to increase invisibility of the watermark (Hsu and Wu, 1999).

The robustness of a watermark can be improved by increasing the energy of the watermark. Increasing the energy, however, degrades the image quality. Thus, to find the best trade-off between the imperceptibility and robustness to signal processing is one of the fundamental issues in digital watermarking.

In literatures, several methods have been proposed to improve the robustness of watermarking algorithms. Podilchuck and Zeng (1998) proposed a similar scheme to Cox et al. (1997) by utilizing a knowledge of human visual systems (HVS) in the DCT domain. By exploiting the masking effects of the HVS, it is possible to hide a watermark with more energy in an image. Therefore, the embedded watermark is highly robust.

Zeng and Lei (1999) proposed a blind DCT-based watermarking algorithm for copyright protection of still image and video data. The characteristics of HVS are exploited in an adaptive image watermarking scheme to achieve high visual quality of the watermarked image and robustness of the watermark.

2.3.2 Wavelet-based image watermarking

Wavelet transform-based image watermarking has multiresolution hierarchical characteristics. It mimics human visual perception and allows an independent processing of transform coefficients in each subband (Kundur and Hatzinakos, 1998). In addition, with the development of the JPEG2000 image compression and MPEG 4 video compression standards, digital watermarking schemes using wavelet transform become attractive to active watermarking research communities.

Xia et al. (1997) introduced a new multiresolution watermarking method based on the discrete wavelet transform (DWT). The watermark modeled by Gaussian noise was added to middle and high frequency bands of a selected image.

Dugad et al. (1998) proposed a spread spectrum image watermarking technique in the discrete wavelet transform domain. They embed a watermark with a constant weighting factor into perceptually significant coefficients in high frequency subbands in order to preserve invisibility. However, it is not robust to common signal processing.

In 2000, the basic idea of Hsu and Wu (1999) is extended to wavelet transform. In watermark embedding process, each decomposed layer of a binary watermark is embedded into a corresponding decomposed layer of an original image. However, embedding the watermark in high frequency components makes this technique fail under an attack of high frequency component removal of the image (Hsu and Wu, 2000).

Yang (2003) has concentrated on the evaluation of biorthogonal wavelets using spread-spectrum watermarking framework.

Another approach of image watermarking is proposed by Wang and Lin (2004). They proposed a wavelet tree quantization for copyright protection watermarking. The wavelet coefficients of the original image are grouped into a predefined structure called supertree. Watermark bits are embedded by quantizing the supertree. Difference between quantized and unquantized trees is then used for watermark extraction.

The wavelet transform provides good spatial-frequency localization. Its multiresolution representation provides a potential tool to model the HVS. Therefore, an efficient relation between transform coefficients and visual masking properties of

the HVS can be constructed. This yields imperceptible and robust watermark (Kurugollu et al., 2003). Accordingly, several papers propose wavelet-based digital watermarking using statistical information of an image and the HVS in order to improve the performance of the watermarking scheme.

Kim and Moon (1999) proposed a robust wavelet-based image watermarking based on statistical information of an image and HVS. An original image is decomposed into 4-level using a DWT. Then, a watermark is embedded into perceptually significant coefficients (PSC) in all subbands, except for the basedband and lowest subbands. The PCS are selected using some statistical characteristics of the image and a scale factor for each subband.

Khamy et al. (2002) introduced a robust technique for image watermarking based on the concept of HVS and wavelet-based data fusion algorithm.

2.3.3 Multiwavelet-based image watermarking

For many years, multi-scale representation and multiresolution analysis have been useful in many image processing applications. Wavelet analysis is a good example to generate such a representation. Another form of the multi-scale representation is generated by using the multiwavelet transform (Strela et al., 1999). Discrete multiwavelet transform (DMT) will be described in more detail in Chapter 3.

In previous works, Kwon and Tewfik (2002) proposed an adaptive image watermarking scheme in the multiwavelet transform domain using successive subband quantization and a perceptual modeling.

Kwon et al. (2002) have extended the idea of Kwon and Tewfik (2002) by using a stochastic visual modeling. This model is based on a noise visibility function (NVF) that uses local image properties for a more robust watermark embedding.

2.4 Artificial Intelligent-Based Image Watermarking

A good robust image watermarking scheme would consist of three key characteristics: perceptual invisibility, robustness and large data capacity (Chang et al., 2005). Unfortunately, these three requirements conflict with one another. Consequently, none of any watermarking scheme is likely to achieve the three characteristics at the same time. One way to solve this problem is to incorporate an explicit HVS model in the watermarking system as previously mentioned.

Another way to improve the performance of watermarking schemes is to employ artificial intelligence (AI) techniques to find the best trade-off between the three conflicting requirements. Embedding a watermark into an image can be expressed as an optimization problem. Therefore, it can be solved by many AI techniques such as genetic algorithms (GA). By literatures, applications of GA to image watermarking problems have not yet been.

Huang and Wu (2002, 2004) proposed a watermarking method based on the DCT and GA. They embed a watermark with visually recognizable patterns into an image by selectively modifying middle-frequency parts of the image. The GA is then applied to search for locations to embed the watermark in each DCT coefficient block such that the quality of the watermarked image is optimized.

Zhang et al. (2002) proposed a novel watermarking scheme for an image, in which a watermark is embedded in the multiwavelet domain of the image using back-propagation neural network (BPN). Due to the learning and adaptive capabilities of BPN, this scheme yields robust watermark.

Shieh et al. (2004) presented a watermarking optimization technique similar to the technique purposed by Huang and Wu (2002, 2004). They use GA to find optimum

frequency bands for embedding a watermark into a DCT-based watermarking system. This scheme simultaneously improves security, robustness of the watermark and image quality.

2.5 Chapter Summary

In this chapter, existing robust image watermarking algorithms found in literature are reviewed. Many of them have been proposed by embedding information either in spatial domain or transform domain. However, watermarking techniques based on the transform domain are more preferable than those based on the spatial domain because higher image quality and more robust watermark can be achieved. In the transform domain watermarking, wavelet transform techniques have been widely used since the discrete wavelet transform provides a hierarchical representation which offers possibility of analyzing a signal at different resolutions. In addition, the DWT plays an important role in the upcoming image and video compression standards. Furthermore, the multiwavelet transform and artificial intelligent techniques have received attention in image watermarking.

CHAPTER III

THEORETICAL BACKGROUNDS

3.1 Introduction

The objective of the research is the development of a new watermarking algorithm for digital image in the multiwavelet transform domain. Therefore, the theoretical backgrounds of multiwavelet and multiwavelet transform are introduced. In addition, a brief introduction to digital watermarking of multimedia content is described. A general framework for watermark insertion and detection is also presented here along with a review of the traditional model of communication systems in order to understand the similarities and differences between watermarking and conventional communications. Basic requirements of digital watermarking are then described in term of perceptual invisibility, robustness and data capacity. After that, performance measures for watermarking algorithm evaluation have been introduced including: peak signal to noise ratio, universal quality index, correlation coefficient, bit error rate and computational complexity. Finally, main applications of digital watermarking are given.

The rest of this chapter is organized as follows: Section 3.2 introduces a theoretical background of multiwavelet and multiwavelet transform. In Section 3.3, a brief introduction to digital watermarking of multimedia content is given. The summary of this chapter can be found in Section 3.4.

3.2 Multiwavelet

The multiwavelet transform is a new concept in the framework of wavelet transforms but has some important differences. In particular, whereas a wavelet has a scaling function and a wavelet function, multiwavelets have two or more scaling functions and appropriate wavelet functions. One of the well-known multiwavelets was constructed by Donovan, Geronimo, Hardin, and Massopust (DGHM) (Geronimo et al., 1994). DGHM multiwavelets simultaneously possess orthogonality, compact support, an approximation order of 2 and symmetry. Next, we give a brief overview of the multiwavelet transform.

3.2.1 Multiwavelet transform

Let Φ denote a compactly supported orthogonal scaling vector $\Phi = (\phi^1, \phi^2, \dots, \phi^r)^T$ where r is the number of scalar scaling functions. Then $\Phi(t)$ satisfies a two-scale dilation equation of the form

$$\Phi(t) = \sqrt{2} \sum_n h(n) \Phi(2t - n) \quad (3-1)$$

for some finite sequence h of $r \times r$ matrices. Furthermore, the integer shifts of the components of Φ form an orthonormal system, that is

$$\langle \phi^l(\cdot - n), \phi^{l'}(\cdot - n') \rangle = \delta_{l, l'} \delta_{n, n'} \quad (3-2)$$

where δ denotes the Kronecker delta function and $\langle \cdot, \cdot \rangle$ denotes the standard inner product.

Let V_0 denote the closed span of $\{\phi^l(\cdot - n) | n \in Z, l = 1, 2, \dots, r\}$ and define $V_j = \{f(\frac{\cdot}{2^j}) | f \in V_0\}$. Then $(V_j)_{j \in Z}$ is a multiresolution analysis of $L^2(R)$.

Note that we choose the decreasing convention $V_{j+1} \subset V_j$.

Let W_j denote the orthogonal complement of V_j in V_{j-1} . Then there exists an orthogonal multiwavelet $\Psi = (\psi^1, \psi^2, \dots, \psi^r)^T$ such that $\{\psi^l(\cdot - n) | l = 1, 2, \dots, r \text{ and } n \in Z\}$ form an orthonormal basis of W_0 . Since $W_0 \subset V_{-1}$, there exists a sequence g of $r \times r$ matrices such that

$$\Psi(t) = \sqrt{2} \sum_n g(n) \Phi(2t - n) \quad (3-3)$$

Let $f \in V_0$, then f can be written as a linear combination of the basis in V_0 :

$$f(t) = \sum_n c_0(k)^T \Phi(t - k) \quad (3-4)$$

for some sequence $c_0 \in l_2(Z)^r$. Since $V_0 = V_1 \oplus W_1$, f can also be expressed as

$$f(t) = \frac{1}{\sqrt{2}} \sum_{k \in Z} c_1(k)^T \Phi\left(\frac{t}{2} - k\right) + \frac{1}{\sqrt{2}} \sum_{k \in Z} d_1(k)^T \Psi\left(\frac{t}{2} - k\right) \quad (3-5)$$

The coefficients c_1 and d_1 are related to c_0 via the following

decomposition and reconstruction algorithm:

$$c_1(k) = \sum_n h(n)c_0(2k+n) \quad (3-6)$$

$$d_1(k) = \sum_n g(n)c_0(2k+n) \quad (3-7)$$

$$c_0(k) = \sum_n h(k-2n)^T c_1(n) + \sum_n g(k-2n)^T d_1(n) \quad (3-8)$$

For the DGHM multiwavelet system, it contains two scaling functions $\phi_1(t)$, $\phi_2(t)$ as shown in Figure 3.1 and two wavelet functions $\psi_1(t)$, $\psi_2(t)$ shown in Figure 3.2. From these figures, it can be seen that DGHM scaling functions and wavelet functions have short support and are symmetric or antisymmetric.

The dilation equation of the DGHM multiwavelet is

$$\Phi(t) = \begin{pmatrix} \phi_1(t) \\ \phi_2(t) \end{pmatrix} = \sum_{n=-2}^1 h(n) \begin{pmatrix} \phi_1(2t-n) \\ \phi_2(2t-n) \end{pmatrix} \quad (3-9)$$

where

$$h(-2) = \frac{1}{20} \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \quad h(-1) = \frac{1}{20} \begin{pmatrix} -3\sqrt{2} & 9 \\ 0 & 0 \end{pmatrix}$$

$$h(0) = \frac{1}{20} \begin{pmatrix} 10\sqrt{2} & 9 \\ 0 & 6\sqrt{2} \end{pmatrix} \quad h(1) = \frac{1}{20} \begin{pmatrix} -3\sqrt{2} & -1 \\ 16 & 6\sqrt{2} \end{pmatrix}$$

The wavelet equation of the DGHM multiwavelet is

$$\Psi(t) = \begin{pmatrix} \psi_1(t) \\ \psi_2(t) \end{pmatrix} = \sum_{n=-2}^1 g(n) \begin{pmatrix} \phi_1(2t-n) \\ \phi_2(2t-n) \end{pmatrix} \quad (3-10)$$

where

$$g(-2) = \frac{1}{20} \begin{pmatrix} 0 & -\sqrt{2} \\ 0 & -1 \end{pmatrix} \quad g(-1) = \frac{1}{20} \begin{pmatrix} -6 & 9\sqrt{2} \\ -3\sqrt{2} & 9 \end{pmatrix}$$

$$g(0) = \frac{1}{20} \begin{pmatrix} 0 & -9\sqrt{2} \\ -10\sqrt{2} & 9 \end{pmatrix} \quad g(1) = \frac{1}{20} \begin{pmatrix} 6 & \sqrt{2} \\ -3\sqrt{2} & -1 \end{pmatrix}$$

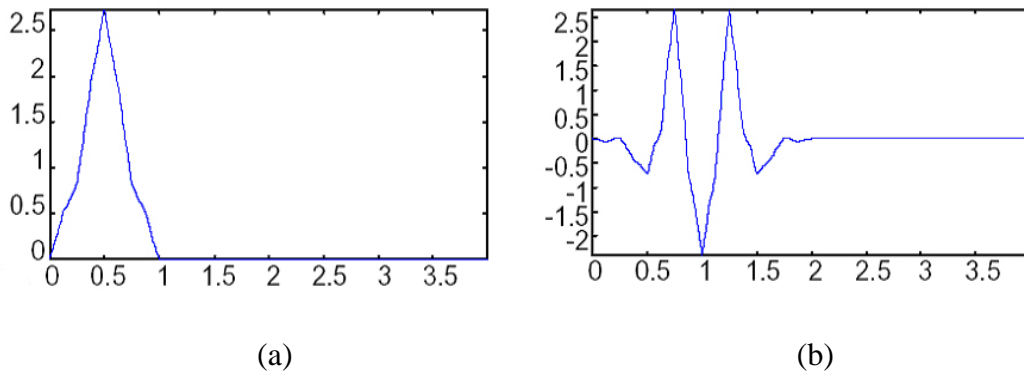


Figure 3.1 DGHM scaling functions (a) $\phi_1(t)$ (b) $\phi_2(t)$.

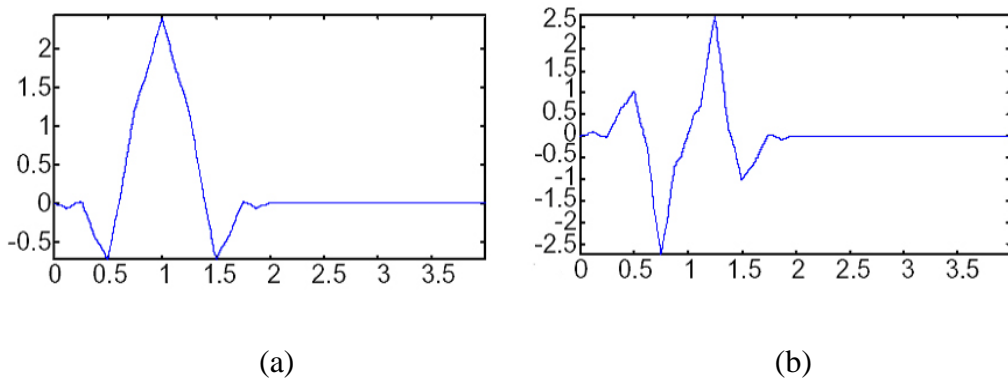


Figure 3.2 DGHM wavelet functions (a) $\psi_1(t)$ (b) $\psi_2(t)$.

Unlike scalar wavelets, even though the multiwavelet is designed to have approximation order p , the filter bank associated with the multiwavelet basis does not inherit this property. Furthermore, since the multiwavelets have more than one scaling function, the dilation equation becomes dilation with matrix coefficients. Thus, in applications, one must associate a given discrete signal to a sequence of length- r vectors (where r is the number of scaling functions) without losing some certain properties of the underlying multiwavelet. Such a process is referred to as prefiltering or multiwavelet initialization. The block diagram of a multiwavelet with prefilter $Q(z)$ and postfilter $P(z)$ is shown in Figure. 3.3. $H(z)$ and $G(z)$ are the z transform of $h(n)$ and $g(n)$, respectively.

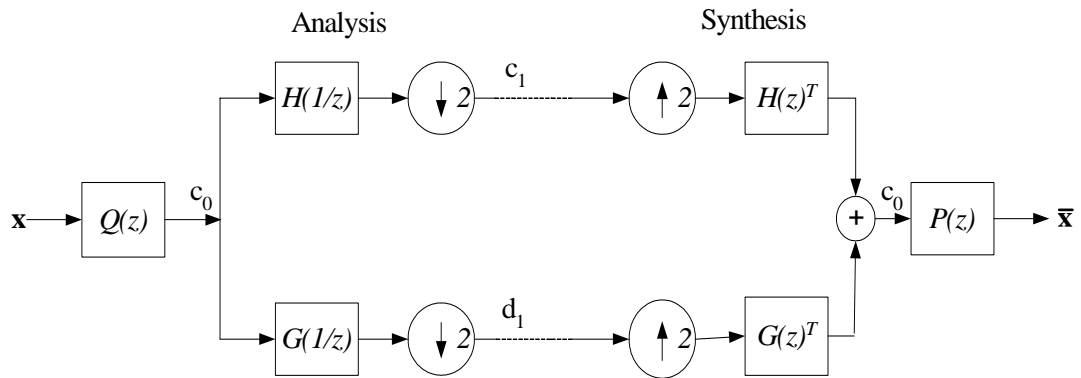


Figure 3.3 Multiwavelet filter bank.

From Figure 3.3, the sequence \mathbf{X} is a vector-valued sequence obtained by the following operator. Define the operator $D_r : R^Z \rightarrow (R^r)^Z$ which partitions a scalar sequence into a sequence grouped in vectors of length r as follows. Given a scalar sequence $x(n)$, $n \in Z$, then $x = D_r(x)$ is given by

$$x = D_r(x) = (\downarrow r) \begin{pmatrix} x(n) \\ x(n+1) \\ \vdots \\ x(n+r-1) \end{pmatrix}_{n \in Z} = \begin{pmatrix} x(rn) \\ x(rn+1) \\ \vdots \\ x(rn+r-1) \end{pmatrix}_{n \in Z} \quad (3-11)$$

Similar to the traditional scalar wavelet transform, the two-dimensional multiwavelet transform can be achieved by applying the one-dimensional transform first on the rows by treating each row as a one-dimensional signal and afterwards on the columns. However, for the applications using multiwavelets, a prefiltering process must be applied to each row and each column to initiate the vector sequence \mathbf{c}_0 to the filter bank (Attakitmongcol et al., 2001).

3.2.2 The recombining processes for the multiwavelet filter bank

An additional step of recombining a vector sequence to a scalar sequence is applied to the output of the analysis filter bank before switching the transform from rows to columns and vice versa. Suppose \mathbf{c} is an output vector sequence from the analysis filter bank and is of the form (Attakitmongcol et al., 2001)

$$\mathbf{c} = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{r1} & c_{r2} & & c_{rn} \end{pmatrix} \quad (3-12)$$

Let c be a scalar sequence obtained from the vector sequence \mathbf{c} . The scalar sequence c can be obtained by either

$$c = (c_{11} \ c_{21} \ \cdots \ c_{r1} \ c_{12} \ c_{22} \ \cdots \ c_{r2} \ \cdots \ c_{1n} \ c_{2n} \ \cdots \ c_{rn}) \quad (3-13)$$

or

$$c = (c_{11} \ c_{12} \ \cdots \ c_{1n} \ c_{21} \ c_{22} \ \cdots \ c_{2n} \ \cdots \ c_{r1} \ c_{r2} \ \cdots \ c_{rn}) \quad (3-14)$$

The recombining methods in (3-13) and (3-14) are referred to as method 1 and method 2, respectively.

Following the recombining method 1 in (3-13), we obtain four image subbands from each level of decomposition; three detail subbands and one approximation subband. For the next level of decomposition, we apply the

multiwavelet transform to the approximation subband of the previous decomposition level, yielding another four subbands. Thus, n levels of decomposition result in $3n + 1$ subbands at the analysis filter bank. Figure 3.4(a) shows the image subbands of single-level decomposition. The three detail subbands are denoted by LH_1 , HL_1 and HH_1 , whereas the approximation subband is denoted by LL_1 . Figure 3.5(a) shows the result of three-level decomposition of the Lena image using the DGHM multiwavelet and recombining method 1.

For the case of the recombining method 2 in (3-14), we obtain image subbands from four orientations as in the previous case but each orientation at each level of decomposition contains $r \times r$ image subbands where r is the number of scaling functions. Thus, n levels of decomposition result in $r^2(3n + 1)$ subbands at the analysis filter bank. Figure 3.4(b) shows the image subbands of single-level decomposition for $r = 2$. In this case, the subband labeled L_1H_2 corresponds to data from the second channel highpass filter in the horizontal direction and the first channel lowpass filter in the vertical direction. The result of applying three-level decomposition using the DGHM multiwavelet and the recombining method 2 to the Lena image is shown in Figure 3.5(b).

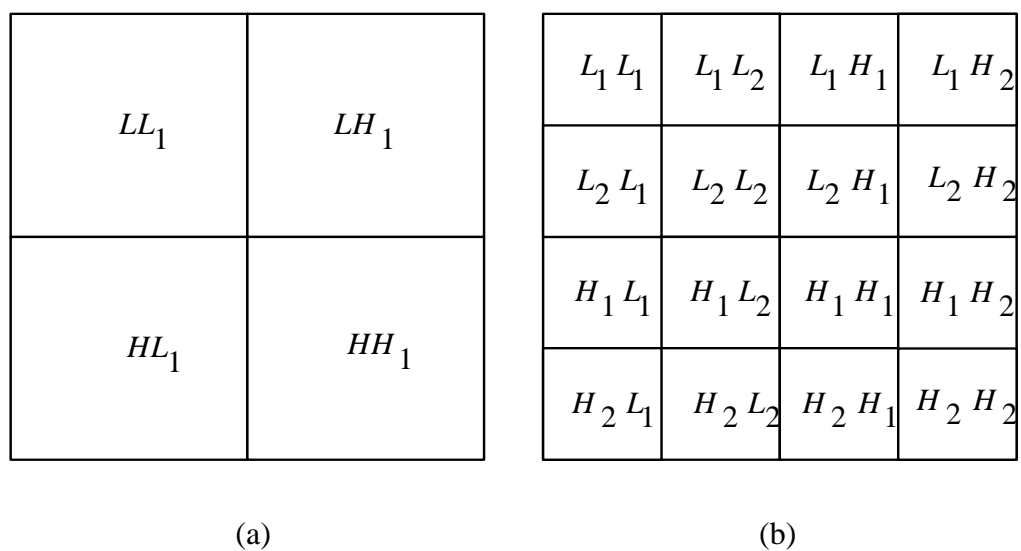


Figure 3.4 Image subbands of single-level decomposition using (a) method 1 and (b) method 2.

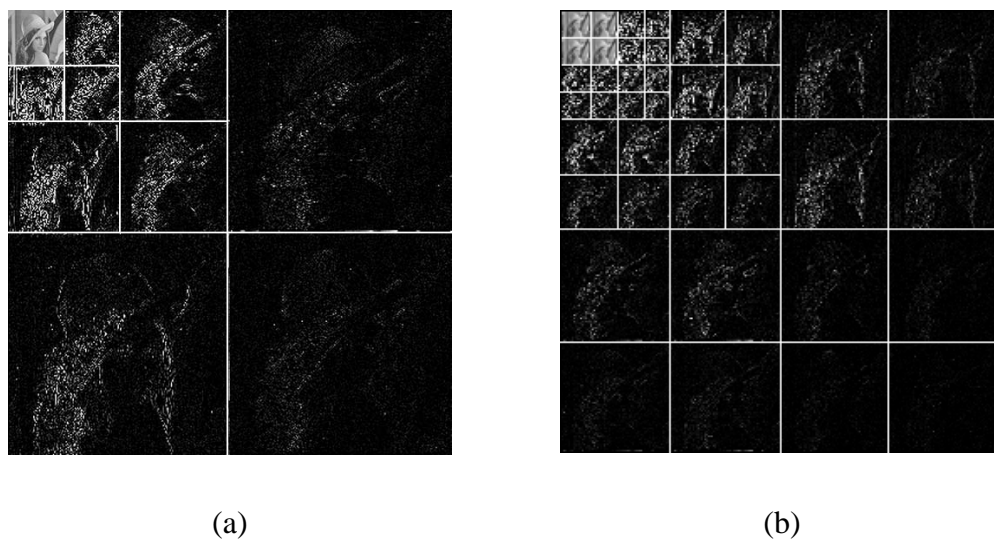


Figure 3.5 Three-level decomposition of the Lena image using the DGHM multiwavelet (with prefiltering) and the recombining (a) method 1 and (b) method 2.

3.3 Digital Watermarking

Digital watermarking of multimedia contents has recently become a very active research area due to the proliferation of digital data and the need to find a solution to protect the copyright of these contents. In recent years, the research community and the industry technology groups began considering digital watermarking technology for inclusion in various standards. The well-known working groups are the Strategic Digital Music Initiative (SDMI) (Kaldenbach, online, 2006) and the Copy Protection Technical Working Group (Bell, 1999). The SDMI is a forum that brings together the worldwide recording, consumer electronics and information technology industries to develop open technology specifications for protected digital music distribution. SDMI is attempting to curb piracy using digital watermarking technology. On the other hand, the CPTWG is concerned with digital video contents stored on digital versatile discs (DVD) which seek to establish a copy protection standard for use with the DVD-Video format. Up to now, to the best of our knowledge, there is no standardization in image watermarking.

Digital watermarking algorithms have been employed for medical images (Giakoumaki et al., 2003), audio (Tefas et al., 2005), video (Barni et al., 2005), graphics (Zafeiriou et al., 2005) and texts (Brassil et al., 1995). Excellent digital watermarking review papers on multimedia watermarking (Hartung et al., 1999; Petitcolas et al., 1999; Langelaar et al., 2000) discuss historic origins of digital watermarking and present several multimedia watermarking algorithms in details.

3.3.1 Digital watermarking framework

This section gives a brief overview of the traditional model of communication systems in order to understand the similarities and differences between watermarking and conventional communications. Then, a general framework for

watermark embedding and watermark detection with different type of watermark detectors which are informed detector and blind detector is presented.

A standard of communication system is the cascade of an information source, a communication link and an information user. The communication link consists of a transmitter, a channel and a receiver. The transmitter modulates or encodes information supplied by the source (input message) into a signal form which is suitable to the channel. The channel conveys the signal over the space intervening between the transmitter and receiver. Then, the receiver demodulates or decodes the signal into a form suitable to the user (output message).

Difference communication channels can be classified according to the type of noise function and how it is applied to the signal. The simplest mathematical model for a communication channel is the additive noise channel (Proakis, 1995), illustrated in Figure 3.6. In this model, transmitted signal $x(t)$ is corrupted by an additive random noise process $n(t)$. In practice, the additive noise process may arise from electronic components or from interference encountered in transmission. If noise is introduced primarily by electronic components and is amplified at the receiver, it may be determined as thermal noise. This type of noise is characterized statistically as a Gaussian noise process. Therefore, the resulting mathematical model for the channel is usually called the additive Gaussian noise channel. Consequently, the received signal is:

$$y(t) = x(t) + n(t) \quad (3-15)$$

Because this channel model is applied to a broad class of physical communication channels and because of its mathematical tractability, this is the predominant channel model used in digital communication system analysis and design. Channel attenuation is easily incorporated into the model. When the signal undergoes attenuation in transmission through the channel, the received signal is

$$y(t) = a \cdot x(t) + n(t) \quad (3-16)$$

where a represents the attenuation factor. The standard model of communication system with an additive noise channel is shown in Figure 3.6.

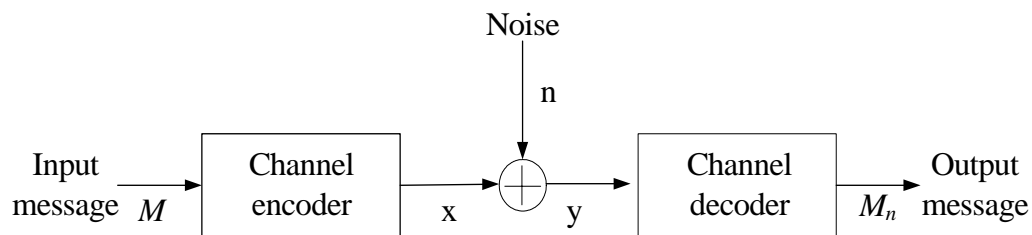
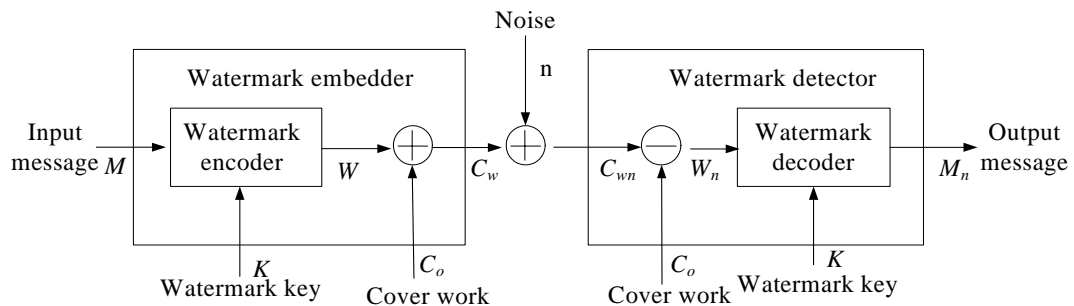


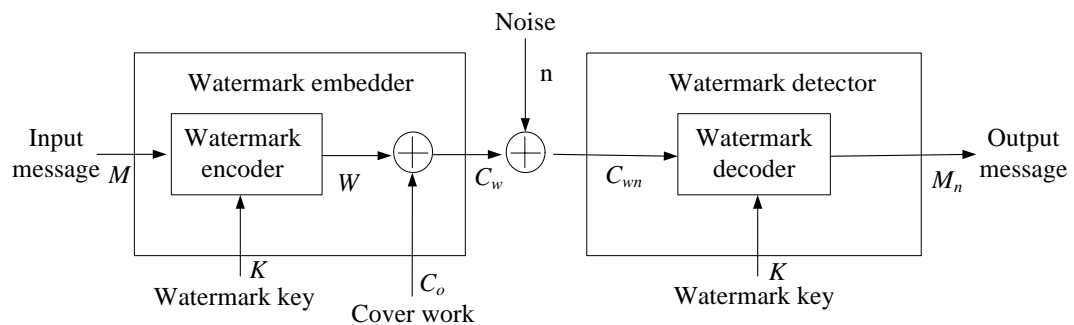
Figure 3.6 Standard model of communication system.

Digital watermarking systems have been modeled as communication systems (Cox et al., 2001). Figure 3.7(a) and Figure 3.7(b) show communication-based models of watermarking that use an informed detector and a blind detector, respectively. In these models, watermarking is viewed as a transmission channel. The cover work C_o , which may be an image, audio or video, is one part of that channel. Note that the original unwatermarked data is referred to as the cover work because it

hides or “covers” the watermark (Cox et al., 2001). In Figure 3.7(a), the watermarking system consists of two main components: watermark embedder and watermark detector. The embedder combines the cover work C_o with the input message M and then creates the watermarked work C_w .



(a)



(b)

Figure 3.7 The model of watermarking systems with (a) informed detector and (b) blind detector.

The embedding operation comprises two steps. First, the watermark encoder takes the input message and maps it into the watermark W , which has to be of the same type and dimension as the cover work. This mapping might be done with a

watermark key K which can be used to enforce the security. Second, the watermark W is added to the cover work to produce the watermarked cover C_w . This operation can be classified as a blind embedder because the encoder ignores the cover work. The embedding operation can be described using the following notations:

$$C_w = f_1(C_o, W) \quad (3-17)$$

and

$$W = f_0(M, K) \quad (3-18)$$

where f_1 and f_0 are embedding function and watermark generating function, respectively.

Another kind of embedder which is contrast to the blind one is an informed embedder. For the informed embedder, the encoder examines the cover work before it creates the watermark. Therefore, the embedding operation can be described using the following notations:

$$C_w = f_1(C_o, W) \quad (3-19)$$

and

$$W = f_0(M, K, C_o) \quad (3-20)$$

In practice, the watermarked cover C_w may be subjected to various types of distortion such as common signal processing, lossy compression and malicious attacks, yielding possibly corrupted watermarked cover C_{wn} . The effect of this processing is modeled as the addition of noise. After the watermarked cover has undergone several distortions, one would like to detect or extract the embedding watermark from the corrupted watermarked cover C_{wn} . Watermark detector either extracts the input message from the corrupted watermarked cover or produces some kind of confidence measure indicating how likely the input message is presented in the data under inspection.

According to the need for original cover work during the watermark detection process, watermark detector can be classified into two categories: informed detector and blind detector. The informed detector, also known as a non-blind detector, uses original cover work in its detection process. On the other hand, the blind detector does not use the original cover. These watermark detectors can be described using the following notation:

$$M_n = g(C_{wn}, K, C_o) \quad (3-21)$$

or without the original cover work C_o ,

$$M_n = g(C_{wn}, K) \quad (3-22)$$

where g is an extracting function.

Note that the watermarking scheme that uses an informed detector is called a private watermarking scheme and the scheme that uses blind detector is called a public or blind watermarking scheme.

3.3.2 Requirements of digital watermarking

Each watermarking application has its own specific requirements. Therefore, there is no set of requirements to be met for all watermarking techniques (Langelaar et al., 2000). Nevertheless, there are some general requirements of the digital watermarking which are presented as follows.

3.3.2.1 Perceptual invisibility

The first requirement is perceptual invisibility. A watermarking algorithm, which satisfies this requirement, must embed the watermark in such a way that it does not affect the quality of the underlying multimedia content.

3.3.2.2 Robustness

The second requirement of watermarking is robustness. The watermark should be resistant to several signal processing. These include compression, geometric transformation, filtering and cropping. In addition, the watermark should be also resistant to intentional attacks that attempt to remove the watermark. However, it is important to note that the level of robustness required varies with respect to applications at hand. For example, fragile watermarks are mainly applied to content authentication and integrity attestation because they are designed to fail when the multimedia content is modified (Langelaar et al., 2000). However, this dissertation generally refers the term “watermark” to imperceptible and robust watermarks.

3.3.2.3 Data capacity

Data capacity or data payload means an amount of information that can be stored in a watermark. Different application has different data payload requirement (Cox et al., 2002). For example, a one-bit watermark is usually sufficient for copy protection propose. For the protection of intellectual property rights, it seems reasonable to assume that one wants to embed an amount of information similar to that used for ISBN (International Standard Book Numbering) or better ISRC (International Standard Recording Code). On top of this, one should also add the year of copyright, the permission grant on the work and the rating for it. This means that roughly 60 bits or 70 bits of information should be embedded into the cover data (Langelaar et al., 2000). This does not include extra bits added for error correction codes.

3.3.2.4 Unambiguity

The last requirement of watermarking schemes is unambiguity. Cox et al (1997) suggested that the retrieval watermark should unambiguously identify the owner. However, the accuracy of identification should degrade gracefully in the case when the watermarked signal is attacked.

3.3.3 Performance measures

The performance of digital watermarking systems depends on the overall watermarking algorithm as well as embedding and detection techniques. Accordingly, the success of a watermarking algorithm is evaluated using a series of measures (Kundur, 1999). This section presents all the most popular metrics to highlight the characteristic of good watermarking scheme. These metrics are described as follows.

3.3.3.1 Peak signal to noise ratio

The Peak Signal to Noise Ratio (PSNR) is an objective visual quality metric. It is the most popular distortion measure in the field of image, video coding and compression. It is widely used due to the simplicity of the metric. However, it is known that the difference distortion metrics are not correlated with human vision. The PSNR between the two images $f(i, j)$ and $g(i, j)$ of $N \times M$ pixels is defined as

$$PSNR = 20 \cdot \log \frac{255}{RMSE} \quad (3-23)$$

where 255 represents the maximum value of luminance and the root mean square error (RMSE) is defined as:

$$RMSE = \sqrt{\frac{1}{N \cdot M} \sum_{i=1}^N \sum_{j=1}^M [g(i, j) - f(i, j)]^2} \quad (3-24)$$

3.3.3.2 Universal quality index

The Universal Quality Index (UQI) is an advanced objective visual quality metric and has been used in benchmarking of image watermarking algorithms for Digital Rights Management (DRM) system (Macq et al., 2004). This quality index is designed by modeling any image distortion as a combination of three factors: loss of correlation, luminance distortion and contrast distortion (Wang et al., 2002). The software to compute the universal quality index is available freely on the Internet and can be downloaded via the HTML link appearing on the reference article.

3.3.3.3 Correlation coefficient

Depending on the type of the watermarking scheme and applications, the watermark detector can produce a number of different outputs. For a one-bit watermarking scheme, the result is just yes/no decision indicating if the copyright holder's watermark has been found in the suspected data. On the other hand, for a multi-bit watermarking scheme, the watermark detector returns the extracted watermarks which are sequence of bits or logo image or copyright information that was hidden in the original data. A widely used similarity measure between the original and the extracted watermark sequences is the normalized correlation coefficient and defined as (Wang and Lin, 2004):

$$\rho(W, \tilde{W}) = \frac{\sum_{i=1}^{N_w} w_i \tilde{w}_i}{\sqrt{\sum_{i=1}^{N_w} w_i^2 \sum_{i=1}^{N_w} \tilde{w}_i^2}} \quad (3-25)$$

where W and \tilde{W} denote an original watermark and extracted one, respectively. N_w is the length of the watermark signal. The extracted yes/no answer can be derived from the correlation $\rho(W, \tilde{W})$ with an appropriate threshold T . If the correlation $\rho(W, \tilde{W})$ is greater than the threshold T , the watermark has been detected otherwise watermark has not been found in the suspected data.

3.3.3.4 Bit error rate

The term “robustness” describes the watermark resistance to some kind of attacks such as common signal processing and compression. For a multi-bit watermarking system, the robustness can be measured by the Bit Error Rate (BER)

which is defined by the ratio of wrong extracted bits to the total number of embedded bits. The bit error rate can also be described using the following equation (Chu et al., 2005):

$$BER = \left(\frac{1}{M_W \cdot N_W} \cdot \sum_{b=1}^{M_W \cdot N_W} (w_b \oplus w'_b) \right) \cdot 100 \% \quad (3-26)$$

where w_b and w'_b represent the embedded watermark bit and the extracted one, respectively. M_W and N_W are the dimensions of the watermark, and \oplus represents exclusive-OR operation.

3.3.3.5 Computational complexity

Computational complexity can be a significant factor in the assessment of feasibility of a watermarking algorithm. However, it depends on the particular application and media being watermarked (Kundur, 1999). For example, in DVD players, watermark extraction must be performed in real-time, but for image watermarking for copyright protection application, it may not be as much concern.

3.3.4 Applications of digital watermarking

The main applications of digital watermarking are described as follows.

3.3.4.1 Copyright protection

The application that attracts the most attention is copyright protection. In this context, a digital watermarking technique embeds a watermark, including a signature or a copyright message, such as a trade logo or a sequence number, into a multimedia content. Subsequently, the watermark can be detected or extracted from the watermarked data and can be adopted to identify its original owner. In order to be efficient, the embedded watermark has to be robust, that is, it has to be

detectable even if the media is processed by common signal processing or any counterfeit attempts.

3.3.4.2 Fingerprinting

Digital fingerprinting is a technology for enforcing digital right policies whereby unique labels, known as digital fingerprints, are inserted into content prior to distribution (Wu et al., 2004). For multimedia content, fingerprints can be embedded using conventional watermarking techniques that are typically concerned with robustness against a variety of attacks. A single digital object can have different fingerprints because they belong to different customers. Therefore, fingerprinting can enable the content owner to identify customers who have broken their license agreement by supplying the data to the third party.

3.3.4.3 Copy protection

In this application, the information stored in a watermark can directly control digital recording devices or perform access control policy. A watermark detector is usually integrated in a compliant recorder or a playback system. Upon watermark detection, the policy is enforced by directing certain hardware or software actions such as disabling a recording module to prevent illegal copying.

3.3.4.4 Broadcast monitoring

Broadcast monitoring is usually used to collect information about the multimedia content being broadcast over the television or radio networks. This information is then used as a base for billing. With the help of the watermarking technology, by embedding watermark in commercial advertisements, an automated monitoring system can verify whether advertisements are broadcasted as contracted.

3.3.4.5 Data authentication

Multimedia editing software, which is available freely on the Internet, makes it easy to alter digital multimedia content. In some applications, such as electronic commerce of multimedia data, medical images, news pictures, it is important to verify whether the content has been modified or not. Fragile watermarks can be used to check the authenticity of the digital multimedia content. They can also be used in applications which are important to figure out how digital content was modified.

3.4 Chapter Summary

This chapter has introduced the theoretical backgrounds of multiwavelet and multiwavelet transform. In addition, the introduction to digital watermarking technology and a general framework of digital watermarking have been presented. The basic requirements of digital watermarking were then described in term of perceptual invisibility, robustness, data capacity and unambiguity. The performance measures for watermarking algorithm evaluation have been introduced. Finally, the issue of watermarking applications is discussed. The main applications of digital watermarking are copyright protection, fingerprinting, copy protection, broadcast monitoring and data authentication. In the next chapter, the effects of transformation methods in image watermarking based on the spread spectrum watermarking framework will be discussed.

CHAPTER IV

EFFECTS OF TRANSFORMATION METHODS ON IMAGE WATERMARKING

4.1 Introduction

This chapter investigates the effects of three different transformation methods including discrete cosine transform, discrete wavelet transform and discrete multiwavelet transform. All transform methods are performed on the same platform using the spread spectrum image watermarking technique. In the spread spectrum watermarking, the watermark insertion is like transmitting a spread spectrum signal (the watermark) through a noisy environment (the original image). We then discuss the experimental results of these three transformation methods.

In the evaluation of watermarking algorithms, we will concentrate on gray scale images because it is easier to compare results and draw conclusions than color images. The performance of each transform-based watermarking scheme is measured by image quality and robustness of the watermark. The robustness is tested after different attacks including JPEG compression with various quality factors, lowpass filtering, Wiener filtering, and adding Gaussian noise.

This chapter is organized as follows. In the next sub-section, we review the work in relative areas. Section 4.2 introduces the spread spectrum image watermarking. In Section 4.3, the experimental results and discussions are given. Finally, the summary of our study can be found in Section 4.4.

4.1.1 Previous works

In general, we can classify digital watermarking into two classes depending on the domain of watermark to be embedded: the spatial domain watermarking and the transform domain watermarking. Currently, watermarking techniques based on transform domain are more popular than those based on spatial domain since they provide higher image quality and much more robust watermark. Therefore, we will concentrate watermarking techniques on transform domain image watermarking.

One of the most cited watermarking schemes in transform domain is proposed by Cox et al. (1997). The authors proposed a watermarking technique by embedding the watermark into the highest magnitude discrete cosine transform (DCT) coefficients of an image using the concept of spread spectrum communication. Since the watermark is embedded into the most perceptually significant regions of the original image, it is tough enough to resist common signal processing and geometric distortions. Xia et al. (1997) introduced a new multiresolution watermarking method based on the discrete wavelet transform (DWT). The watermark is embedded to some of the large wavelet coefficients at high and middle frequency bands of the image's DWT. Song et al. (2000) gave the comparison of different watermarking techniques by focusing on the evaluation of robustness and visual quality property. S. H. Yang (2003) has concentrated his work on the evaluation of biorthogonal wavelets using spread-spectrum watermarking framework.

4.2 Evaluation Method

This work is focused on the study of watermarking on images for copyright

protection applications. We investigate the effects of different types of transformations in image watermarking by using Cox's algorithm (Cox et al., 1997). The main motivation of using Cox's algorithm is that it is the first transform domain watermarking algorithm and is well-known to the watermarking communities (Meerwald and Pereira, 2002). Moreover, this algorithm is often used as a reference method in the design of watermarking algorithms (Lumini and Maio, 2000; Zhang et al., 2000; Liu and Tan, 2000). It is referred to as private watermarking scheme since it needs the original image during the watermark extraction process.

4.2.1 Spread spectrum image watermarking

Spread-spectrum communication is a popular analogy for watermarking. The well-known spread-spectrum watermarking technique is proposed by Cox et al. (1997). For this technique, the embedding procedure is like transmitting a spread spectrum signal (the watermark) through a noisy environment (the original image). Watermark extraction is equivalent to the detection of the spread spectrum signal from an interference environment.

4.2.1.1 Watermark embedding algorithm

The watermark embedding algorithm is as follows:

1. We transform an original image using the discrete cosine transform (DCT). In order to trade off between robustness and invisibility, the watermark is embedded to the 1,000 largest coefficients, except for DC (direct current) coefficient.
2. The watermark to be embedded is a sequence of 1,000 random numbers, having a Gaussian (normal) distribution with zero mean and unit variance. The encoding function can be expressed as (Cox et al., 1997):

$$V_i' = V_i + \alpha V_i X_i \quad (4-1)$$

where V_i is the selected DCT coefficients, X_i is the watermark and α is the embedding strength.

3. The watermarked image is obtained by the inverse DCT of V_i' . The watermark embedding process by using DCT is shown in Figure 4.1.

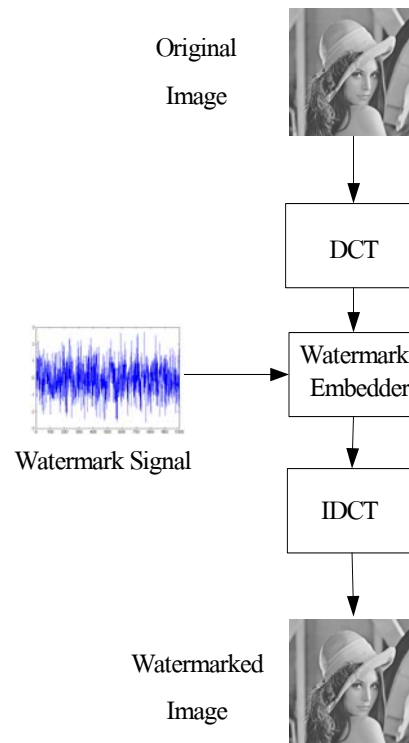


Figure 4.1 Watermark embedding process by using DCT.

4.2.1.2 Watermark extracting algorithm

The watermark extraction is the inverse procedure of the watermark insertion process. The watermark extraction algorithm is as follows:

1. We first transform a watermarked image and the original image with DCT. Then, the watermark is obtained by subtracting the original image coefficients from the watermarked image coefficients.

2. After extracting the watermark, similarity between the original watermark and the extracted watermark is taken as a measurement of presence of the watermark. A similarity between X and X^* is defined as (Cox et al., 1997):

$$sim(X, X^*) = \frac{X \cdot X^*}{\sqrt{X^* \cdot X^*}} \quad (4-2)$$

where X is the original watermark and X^* is the extracted watermark.

3. To decide whether the suspected image is a watermarked version of the original image, the similarity is compared with a pre-specified threshold δ . If the similarity is greater than the pre-specified threshold, the watermark has been detected.

4. In Cox et al. (1997), it was shown that $sim(X, X^*)$ follows the standard Gaussian distribution of zero mean and unit variance. Thus, the probability of false alarm in watermark detection can be estimated as follows (Miller and Bloom, 1999):

$$p = \frac{1}{\sqrt{2\pi}} \int_{\delta}^{\infty} e^{-\frac{1}{2}t^2} dt \quad (4-3)$$

Setting the threshold $\delta = 6$ yields the high reliability of the watermark detection scheme such that probability of false alarm is less than 9.8659×10^{-10} . The watermark extracting process is shown in Figure 4.2.

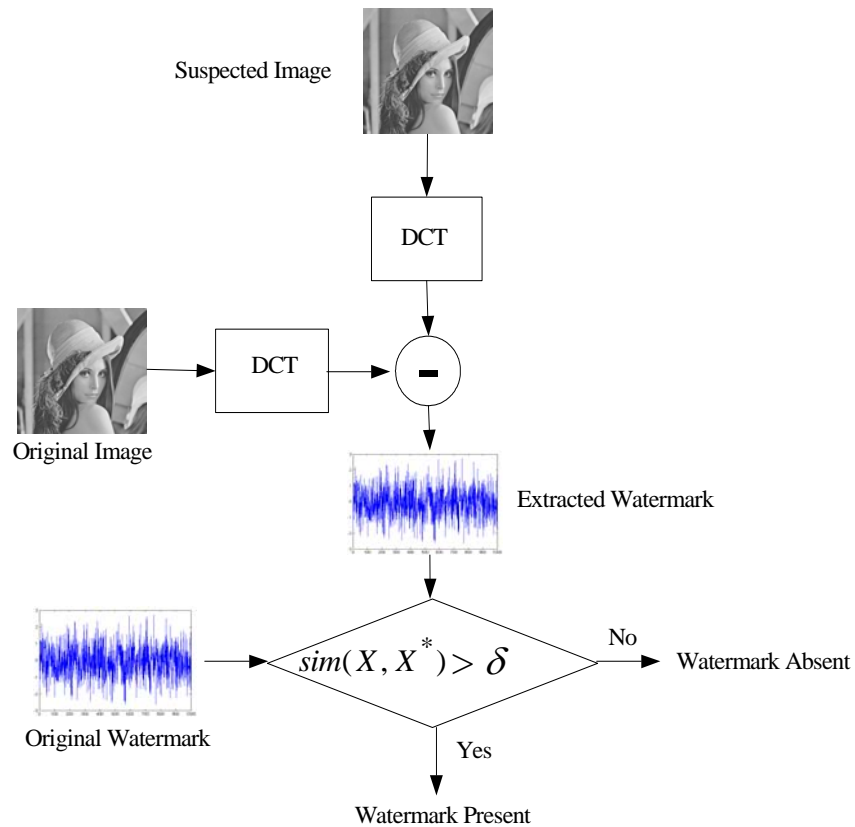


Figure 4.2 Watermark extracting process by using DCT.

4.3 Results and Discussions

In this section, some experimental results are demonstrated to show the effects of three transformations on the spread spectrum image watermarking technique. All of the original test images are gray-scale standard images of size 512×512 pixels obtained from the Waterloo BragZone (2004) and the SIPI image database (2004). To study the effects of transformation methods, we perform the same watermark insertion and watermark detection based on Cox's algorithm with various transformation methods. For the cases of using DWT and DMT, we decompose an original image into 3 levels and the watermark is embedded to the 1,000 largest coefficients of all subbands, except for approximation subband (LL_3). The DWT and DMT coefficients are modeled using the Gaussian distribution with zero means and variances that depend on the coefficient location in each subband (Joshi et al., 1997; Cheng and Huang, 2003). Figures 4.3(a) - 4.3(d) show the original Lena image and its transformed coefficients using DCT, DWT and DMT respectively. The performance of each transform-based watermarking scheme is measured by image quality and robustness of the watermark.

4.3.1 Imperceptibility

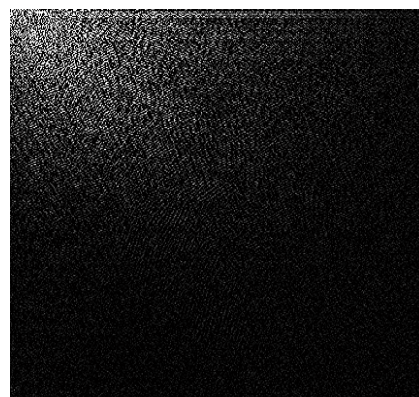
Imperceptibility of watermarking algorithm means that the watermark should be embedded into the original image without causing any significant visual degradation. To measure the image quality of the watermarked image, we use the peak signal to noise ratio (PSNR). In this simulations, the embedding strength is 0.1 (a typical value used by Cox et al. (1997)). In Figures 4.4(a), 4.5(a) and 4.6(a) show the watermarked versions of the Lena image from three methods. We can see that most of the watermarked images are not perceptually different from the original ones, but the

absolute difference between the original image and the watermarked image using DCT can be clearly seen. The absolute differences between the original image and the watermarked ones, magnified by a factor 8 are shown in Figures 4.4(b), 4.5(b) and 4.6(b), for DCT, DWT, and DMT methods, respectively. In cases of DWT and DMT methods, it is evident that the watermark is mainly hidden into the high activity regions and around the edges which are less sensitive to human eyes than the low activity regions. Therefore, these methods produce high image quality than the one using DCT method. The experimental results of image quality measured by PSNR are shown in Table 4.1.

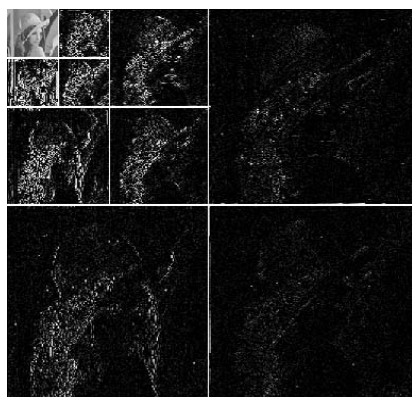
The PSNR of the watermarked image with various embedding strengths is illustrated in Figure 4.7. From Figure 4.7, the results clearly show that the method using DMT yields the best image quality.



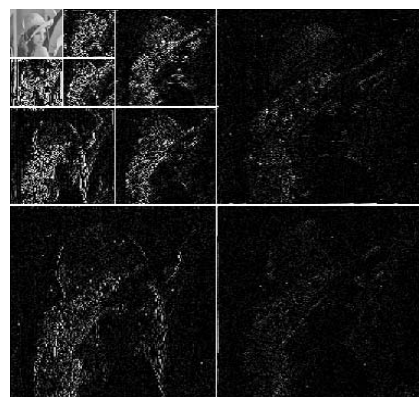
(a)



(b)



(c)



(d)

Figure 4.3 (a) Original “Lena” image and transformed coefficients using the (b) DCT, (c) DWT and (d) DMT.



Figure 4.4 (a) Watermarked “Lena” image using DCT method and
(b) absolute difference between the original image and
the watermarked image, magnified by a factor 8.



Figure 4.5 (a) Watermarked “Lena” image using DWT method and
(b) absolute difference between the original image and
the watermarked image, magnified by a factor 8.



Figure 4.6 (a) Watermarked “Lena” image using DMT method and
(b) absolute difference between the original image and
the watermarked image, magnified by a factor 8.

Table 4.1 PSNR of watermarked images using 5 test images.

Image	PSNR (dB)		
	DCT	DWT	DMT
Lena	36.46	47.35	49.37
Baboon	37.40	40.69	47.23
Gold Hill	34.44	46.42	48.88
Boat	36.25	44.35	47.15
Peppers	33.71	45.28	47.01

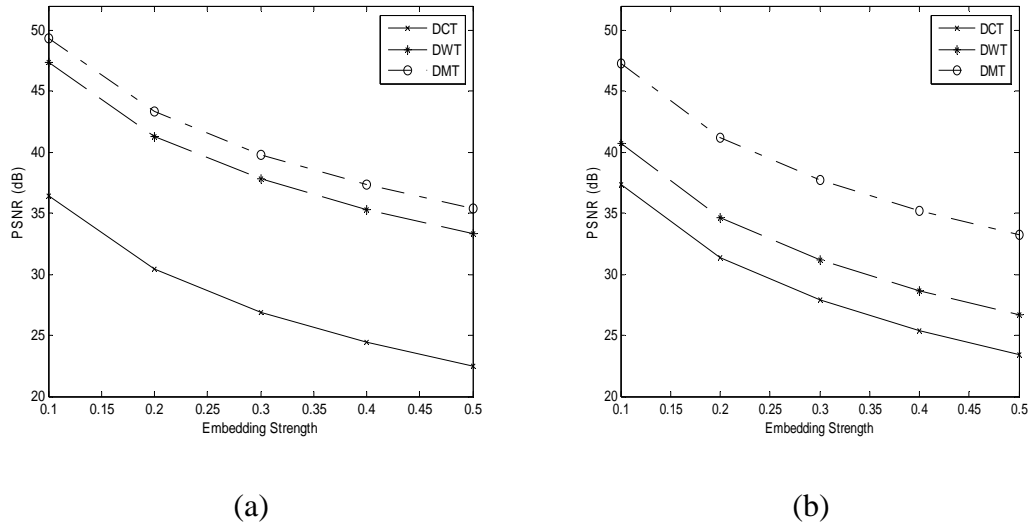


Figure 4.7 PSNR of (a) Lena and (b) Baboon watermarked images with different watermark strengths.

4.3.2 Robustness

Robustness of the watermark means that the watermark must be difficult to be removed by an attacker trying to counterfeit the copyright of the image. Any attempts to remove or destroy watermark should produce a remarkable degradation in image quality before the watermark is lost. In particular, the watermark should be resistant to common signal processing techniques and lossy compression.

In order to compare robustness between these three techniques, the parameters for each scheme should be adjusted so that watermarked images of approximately the same imperceptibility are produced. In these experiments, the PSNR of watermarked image in each scheme was set to 43 dB. This was done by selecting the appropriate embedding strength using Newton's root-finding method (Etter and Ingber, 2003). The embedding strengths according to this PSNR value are shown in Table 3.2.

Table 4.2 Embedding strengths of watermark signal for the test images.

Images	Transformation methods		
	DCT	DWT	DMT
Lena	0.0471	0.2210	0.2082
Baboon	0.0525	0.1670	0.1628

To verify the detecting uniqueness, we send the extracted watermark together with other 1,000 random watermarks to the correlation detector. The 500th watermark is the extracted watermark. From Figure 4.8, we can see that the detector response of the real watermark is very high while other responses are very low.

JPEG compression is among the well known compression standards. The quality of the compression refers to the amount of compression and thus amount of degradation. The quality parameters are in the range from 0 to 100 %, where zero quality compression is the best in saving space but results in the most distortion on the image. To verify the robustness of the watermark under lossy image compression, we compressed watermarked image using JPEG compression with quality factors varying from 10% to 100%. The similarities of the original and extracted watermarks are shown in Figures 4.9(a) and 4.9(b) for Lena and Baboon images, respectively. We can see that the algorithm using DMT gives the most robust watermark.

To evaluate the robustness of the watermark under common signal processing, we apply different types of attacks including lowpass filtering, Wiener filtering and adding Gaussian noise. Figure 4.10 shows the similarities of watermarks when the watermarked image is attacked by lowpass filtering. We can see that all

methods have little resistance to this kind of attack. However, the method using DCT yields the most robust watermark.

Next, the robustness of the watermark is tested by using Wiener filtering. The result in Figure 4.11 shows that the methods using DWT and DMT give almost the same robust watermark to this kind of attack. Moreover, these two methods yield more robust watermark than the one using DCT.

Finally, we examine the robustness against noise addition attacks. In many cases, the degradation and distortion of the image come from noise addition. In our experiment, we add Gaussian noise of mean 0 and variance 500 to the watermarked image and perform watermark extraction. The experiment result in Figure 4.12 shows that the algorithm using DMT produces the most robust watermark for this kind of attack.

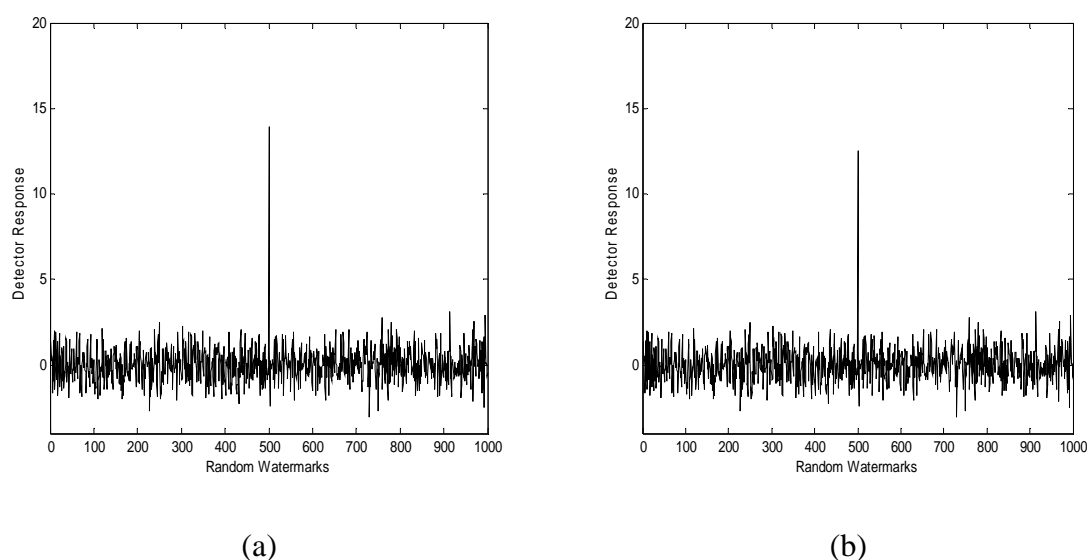


Figure 4.8 Detector response of 1,000 watermarks including extracted watermark of

(a) Lena image and (b) Baboon image using DCT under 10 % JPEG quality.

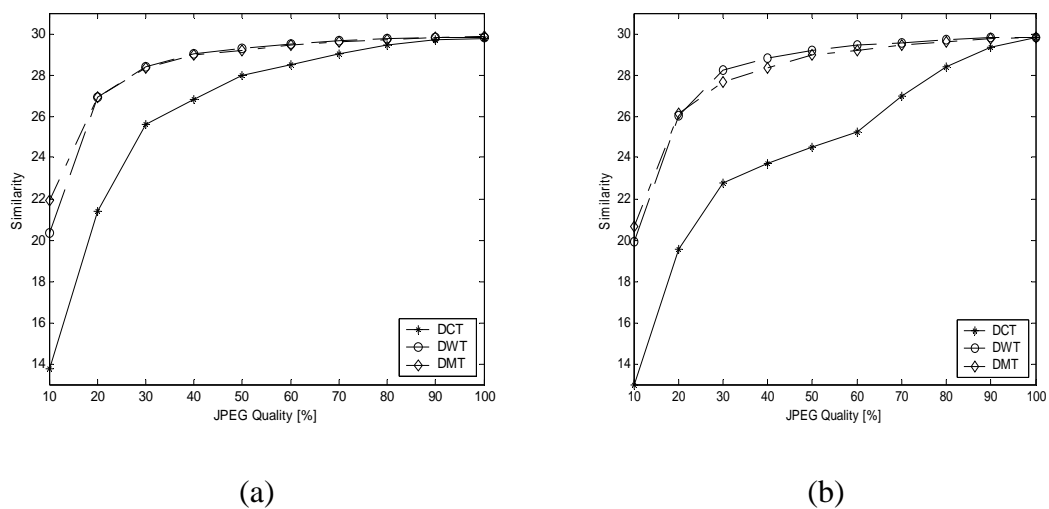


Figure 4.9 Similarities of watermarks under JPEG compression (a) Lena and (b) Baboon images.

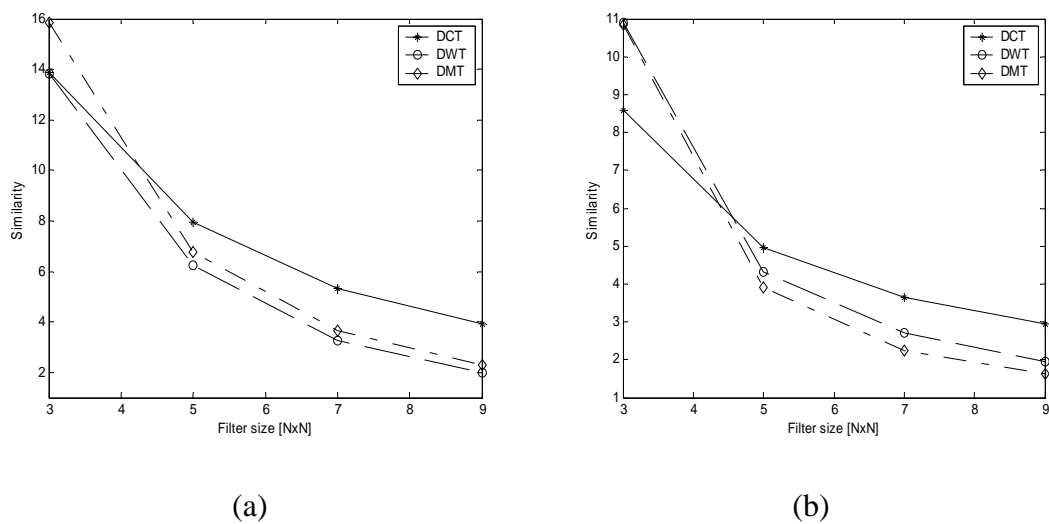
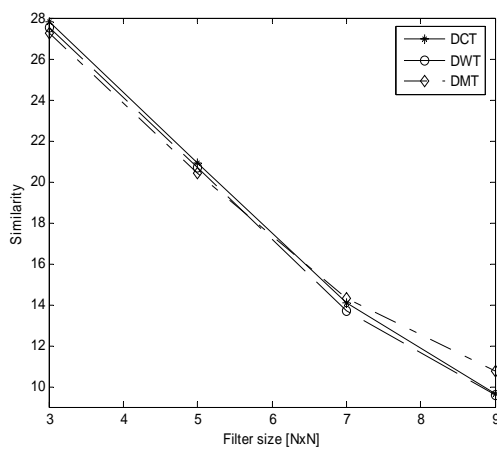
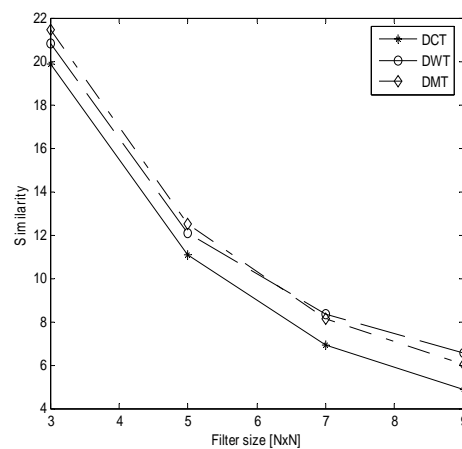


Figure 4.10 Similarities of watermarks under lowpass filtering (a) Lena and (b) Baboon images.

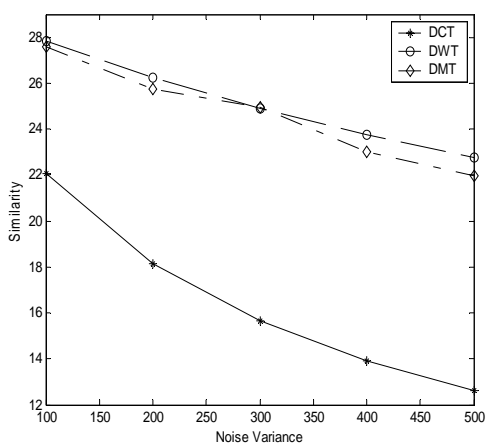


(a)

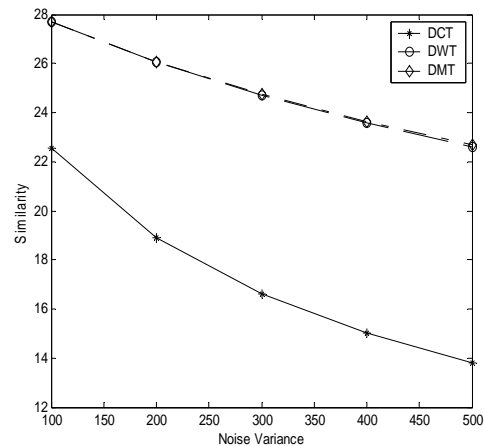


(b)

Figure 4.11 Similarities of watermarks under Wiener filtering (a) Lena and (b) Baboon images.



(a)



(b)

Figure 4.12 Similarities of watermarks under Gaussian noise addition (a) Lena and (b) Baboon images.

4.4 Chapter Summary

In this chapter, we have studied the effects of transformations including the discrete cosine, discrete wavelet and discrete multiwavelet transforms in the spread spectrum image watermarking algorithm. Due to the multiresolution representation obtained from using DWT and DMT, the algorithms using both transforms yield better image quality than the one using DCT. However, the algorithm using DMT gives the most robust watermark under JPEG compression and common signal processing except for lowpass filtering. This is likely due to the fact that for the watermarking in the DCT domain, watermark spreads over a set of visually important frequency components. Further research can be focused on the development of robust watermarking method using the multiwavelet transform which can survive JPEG compression and common signal processing including lowpass filtering attack.

CHAPTER V

EFFECTS OF THE RECOMBINING PROCESSES FOR THE MULTIWAVELET FILTER BANK ON IMAGE WATERMARKING

5.1 Introduction

Multiwavelet transform has received attention in image watermarking because it is possible to construct multiwavelets that simultaneously possess desirable properties. Since the choice of recombining processes for the multiwavelet filter bank is a critical issue that affects the quality of the watermarked image and the robustness of the watermark, we selected two different watermarking algorithms in this chapter to evaluate their performances in order to choose the best recombining method for our multiwavelet based image watermarking algorithm. One is a public watermarking scheme and the other is a private watermarking scheme. The evaluation is performed under a spread spectrum image watermarking framework from the view point of robustness of the watermark. The attacks include JPEG compression with different quality factors, lowpass filtering, Wiener filtering, and Gaussian noise addition.

This chapter is organized as follows. In the next sub-section, we review the work in relative areas. Section 5.2 reviews some background of recombining processes for the multiwavelet filter bank. In Section 5.3, the experimental results and discussions are given. Finally, the chapter summary can be found in Section 5.4.

5.1.1 Previous works

Digital image watermarking provides copyright protection of image data by hiding appropriate information in the original image. This must be performed in such a way that the added information does not cause degradation of the perceptual image quality and cannot be removed. In general, we can classify digital watermarking into two classes depending on the domain of watermark embedding, i.e. the spatial domain and the transform domain, where the properties of the underlying domain can be exploited. Currently, watermarking techniques based on transform domain are more popular than those based on spatial domain since they provide higher image quality and much more robust watermark (Hartung and Kutter, 1999; Petitcolas et al., 1999; Song and Tan, 2000). According to the need for original data during the watermark detection process, digital watermarking can also be classified into private and public (or blind) algorithms. Private methods need the original data during the detection process. In some cases when the original data is not easy to obtain or when we do not know which copy is the original one, it is necessary to use blind watermarking for resolving rightful ownership.

In previous research, Dugad et al. (1998) proposed the spread spectrum image watermarking technique in the discrete wavelet transform (DWT) domain. They embed a watermark with a constant weighting factor into the perceptually significant coefficients in the high frequency subbands in order to preserve invisibility. However, it is not robust to common signal processing. Consequently, the development of a new algorithm that can satisfy both invisibility and robustness is needed. In 2002, El - Khamy et al. (2002) introduced a robust technique for image watermarking based on the concept of Human Visual System (HVS) and wavelet-based data fusion algorithm.

Kwon and Tewfik (2002) proposed an adaptive image watermarking scheme in the multiwavelet transform domain using successive subband quantization and a perceptual modeling. Kwon et al. (2002) have extended the idea of Kwon and Tewfik (2002) by using a stochastic visual modeling. This model is based on a noise visibility function (NVF) that uses local image properties for watermark embedding.

5.2 Evaluation Method

This section will elaborate on the proposed approach in details.

5.2.1 The recombining processes for the multiwavelet filter bank

Similar to the traditional scalar wavelet transform, the two-dimensional multiwavelet transform can be achieved by applying the one-dimensional transform first on the rows by treating each row as a one-dimensional signal and afterwards on the columns. However, for the applications using multiwavelets, a prefiltering process must be applied to each row and each column to initiate the vector sequence to the multiwavelet filter bank. Furthermore, an additional step of recombining a vector sequence to a scalar sequence is applied to the output of the analysis filter bank before switching the transform from rows to columns and vice versa. Suppose \mathbf{c} is an output vector sequence from the analysis filter bank and is of the form (Attakitmongcol et al., 2001)

$$\mathbf{c} = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{r1} & c_{r2} & & c_{rn} \end{pmatrix} \quad (5-1)$$

Let c be a scalar sequence obtained from the vector sequence \mathbf{c} . The scalar sequence c can be obtained by either

$$c = (c_{11} \ c_{21} \ \dots \ c_{r1} \ c_{12} \ c_{22} \ \dots \ c_{r2} \ \dots \ c_{1n} \ c_{2n} \ \dots \ c_{rn}) \quad (5-2)$$

or

$$c = (c_{11} \ c_{12} \ \dots \ c_{1n} \ c_{21} \ c_{22} \ \dots \ c_{2n} \ \dots \ c_{r1} \ c_{r2} \ \dots \ c_{rn}) \quad (5-3)$$

The recombining methods in (5-2) and (5-3) are referred to as method 1 and method 2, respectively.

Following the recombining method 1 in (5-2), we obtain four image subbands from each level of decomposition; three detail subbands and one approximation subband. For the next level of decomposition, we apply the multiwavelet transform to the approximation subband of the previous decomposition level, yielding another four subbands. Thus, n levels of decomposition result in $3n + 1$ subbands at the analysis filter bank. Figure 5.1(a) shows the image subbands of single-level decomposition. The three detail subbands are denoted by LH_1 , HL_1 and HH_1 , whereas the approximation subband is denoted by LL_1 . Figure 5.2(a) shows the result of three-level decomposition of the Lena image using the DGHM multiwavelet and recombining method 1.

For the case of the recombining method 2 in (5-3), we obtain image subbands from four orientations as in the previous case but each orientation at each level of decomposition contains $r \times r$ image subbands where r is the number of

scaling functions. Thus, n levels of decomposition result in $r^2(3n+1)$ subbands at the analysis filter bank. Figure 5.1(b) shows the image subbands of single-level decomposition for $r = 2$. In this case, the subband labeled L_1H_2 corresponds to data from the second channel highpass filter in the horizontal direction and the first channel lowpass in the vertical direction. The result of applying three-level decomposition using the DGHM multiwavelet and the recombining method 2 to the Lena image is shown in Figure 5.2(b).

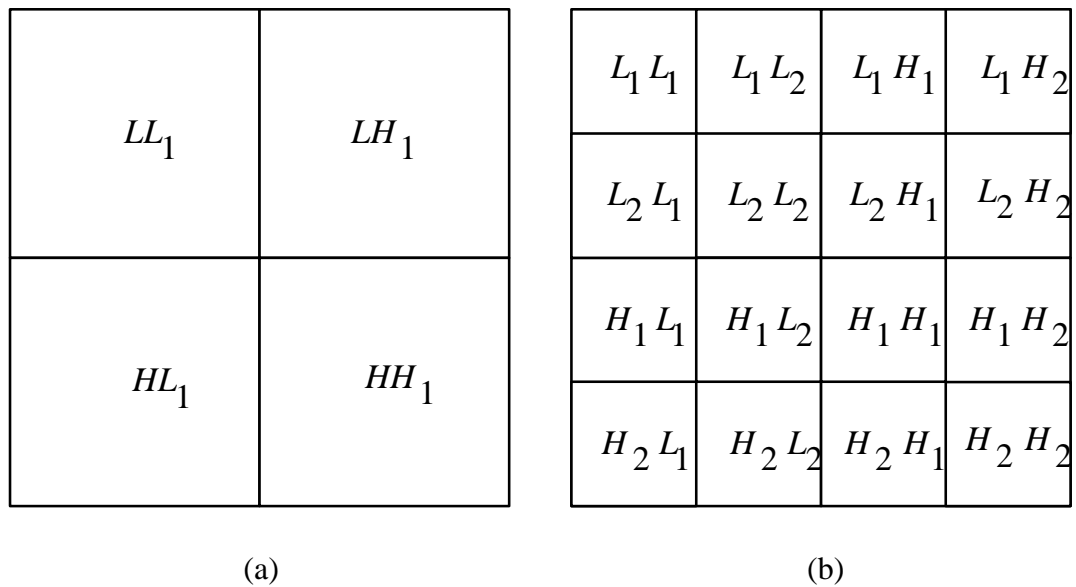


Figure 5.1 Image subbands of single-level decomposition using (a) method 1 and (b) method 2.

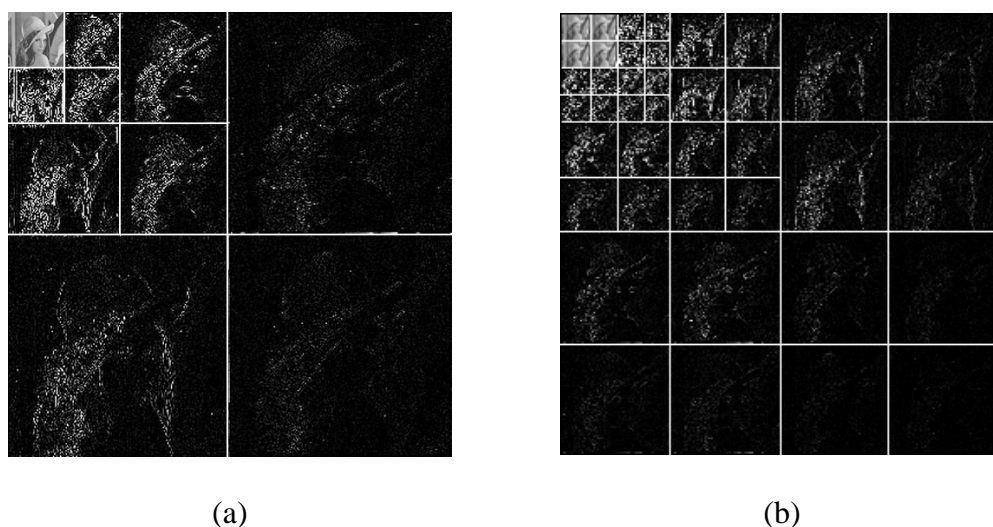


Figure 5.2 Three - level decomposition of the Lena image using the DGHM multiwavelet (with prefiltering) and the recombining (a) method 1 and (b) method 2.

As a result, we have two recombining processes for the multiwavelet filter bank. In order to choose the recombining method for our watermarking algorithm, we perform two simulations on spread spectrum image watermarking techniques using a public watermarking scheme and private one. All of the original test images are gray-scale standard images of size 512×512 pixels obtained from the Waterloo BragZone (2004) and the SIPI image database (2004).

5.2.2 Public watermarking scheme

In this section, the public watermarking scheme is described with a particular attention to the method proposed by Dugad et al. (1998).

5.2.2.1 Watermark embedding algorithm

The watermark embedding algorithm is as follows:

1. Transform the original image into 3-level decomposition using the DGHM multiwavelet and optimal orthogonal prefilter from Attakitmongkol et al. (2001).

2. Since the approximation subband contains the high-energy components of the image, we do not embed the watermark in this subband to avoid visible degradation of watermarked image. In other subbands, we choose all DMT coefficients which are greater than the embedding threshold T_1 . These coefficients are named V_i and applied to the following equation:

$$V_i' = V_i + \alpha |V_i| x_i \quad (5-4)$$

where i runs over the wavelet coefficients V_i and V_i' denotes the coefficients of the watermarked image. The variable x_i is the watermark signal which is generated from a Gaussian distribution with zero mean and unit variance and α (ALPHA) is the embedding strength used to control the watermark energy.

3. Pass the modified DMT coefficients through the inverse DMT to obtain the watermarked image. The watermark embedding process is shown in Figure 5.3.

5.2.2.2 Watermark detection algorithm

The watermark detection algorithm is as follows:

1. For watermark detection, the suspected image is decomposed into 3 levels using the DMT. We choose all the DMT coefficients greater than the detection threshold T_2 from all subbands except the approximation subband

and the subbands of the finest scale. These coefficients are referred to as \tilde{V}_i . The detection threshold T_2 must be strictly larger than embedding threshold T_1 for robustness of the watermark since some coefficients which were originally below T_1 may become greater than T_1 due to image manipulations.

2. We compute the correlation z between the coefficients \tilde{V}_i and the original copy of the watermark using the following equation:

$$z = \frac{1}{M} \sum_i \tilde{V}_i x_i \quad (5-5)$$

where i runs over the wavelet coefficients \tilde{V}_i and M is the number of the coefficients \tilde{V}_i . Since x_i and \tilde{V}_i are independent random variables, the product $\tilde{V}_i x_i$ is also an independent random variable. Thus, by applying the central limit theorem (Papoulis, 1965) for the correlation z , the distribution of the correlation z tends towards standard Gaussian distribution.

3. To examine the existence of the embedded watermark for identification of the ownership, we compare the correlation z with the threshold S described by

$$S = \frac{\alpha}{2M} \sum_i |\tilde{V}_i| \quad (5-6)$$

If the correlation z is greater than the threshold S , the watermark has been detected.

More details on the threshold selection analysis can be found in Inoue et al. (1999).

4. We compute the correlation output which is the ratio of the number of subbands that have been found to have watermark and the number of subbands that have the coefficients $> T_2$. For example, if we detect the watermark in 8 subbands from the total of 9 subbands that have the coefficients $> T_2$, then the correlation output is 8/9. The watermark detection process is shown in Figure 5.4.

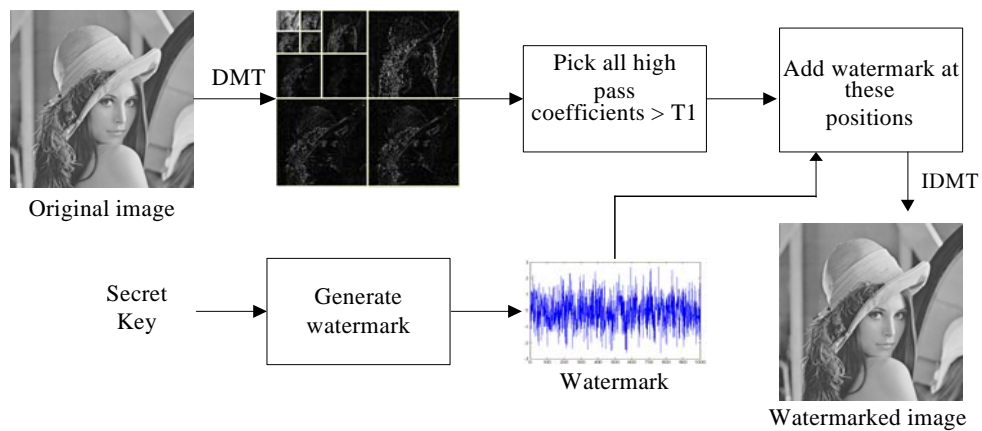


Figure 5.3 Watermark embedding process.

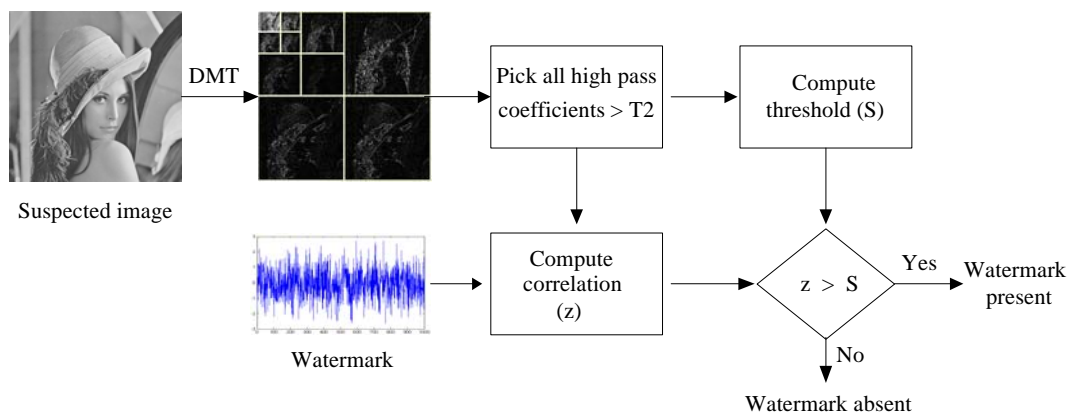


Figure 5.4 Watermark detection process.

5.3 Results and Discussions

In this section, some experimental results are demonstrated to show the effects of the recombining processes for the multiwavelet filter bank on image watermarking. The entire original test images are gray-scale standard images of size 512×512 pixels obtained from the Waterloo BragZone (2004) and the SIPI image database (2004). The performances of a public watermarking scheme and private one are measured by the robustness of the watermark. The attacks include JPEG compression, lowpass filtering, Wiener filtering, and Gaussian noise addition.

5.3.1 Results of the private watermarking scheme

We investigate the effects of the recombining processes for the multiwavelet filter bank on the private watermarking scheme using the spread spectrum image watermarking technique proposed by Cox et al. (1997) as described in the previous chapter. In our simulations, we decompose an original image into 3 levels using the DMT and the watermark is embedded to the 1,000 largest coefficients of all subbands, except for the approximation subband. The watermark consists of a sequence of 1,000 randomly generated real numbers having a Gaussian distribution with zero mean and unit variance. For a fair comparison, the peak signal to noise ratio (PSNR) of the watermarked image was set to 43 dB. This was achieved by selecting the appropriate embedding strength using Newton's root-finding method (Etter and Ingber, 2003).

We evaluate and compare the performances of both recombining methods to various types of image distortions. As in Chapter 4, the similarity between the embedded and extracted watermarks, given by Equation (4-2), is computed to assess robustness. A similarity threshold of 6.0 which corresponds to a probability of false

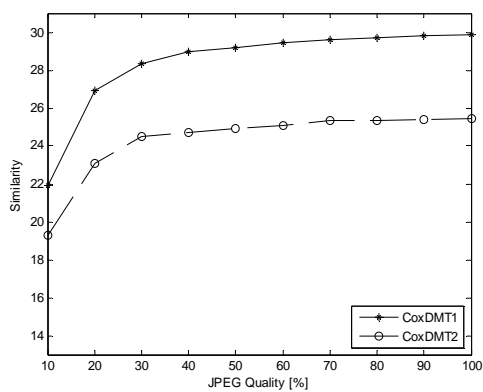
alarm less than 9.8659×10^{-10} for 1,000 random watermarks is employed. The results obtained from using recombining methods 1 and 2 are called CoxDMT1 and CoxDMT2, respectively.

In the first experiment, JPEG compression with various quality factors was applied to the watermarked image. The robustness of the watermark under JPEG compression with quality factors varying from 10% to 100% using Lena and Baboon images are shown in Figure 5.5. We can see that both schemes are robust against this attack and the CoxDMT1 method gives more robust watermark.

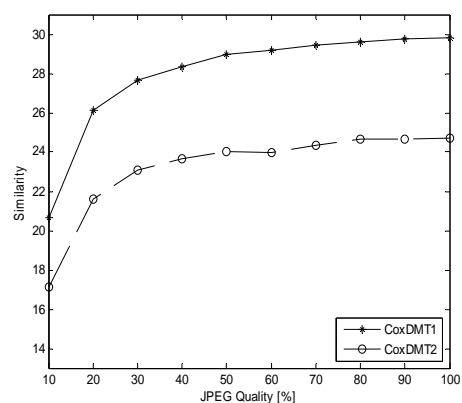
Next, lowpass filtering and Wiener filtering were used to test the robustness of the watermarking schemes. As shown by the results in Figures 5.6 and 5.7, the CoxDMT1 yields better results than the CoxDMT2.

Finally, the robustness of the watermarking schemes was tested against adding Gaussian noise. As shown by the results in Figure 5.8, both schemes are robust against noise addition and the CoxDMT1 yields better results than the CoxDMT2.

The experiment results clearly show that the recombining method 1 gives more robust watermark than method 2. This is because for the recombining method 1 which produces fewer subbands than method 2, the high-magnitude coefficients are likely to be in the same subbands. Thus, the algorithm using recombining method 1 is able to embed the watermark signal to more number of high-magnitude coefficients than the one using recombining method 2. As a result, the watermark from the algorithm using recombining method 1 is more robust than the one from the algorithm using method 2.

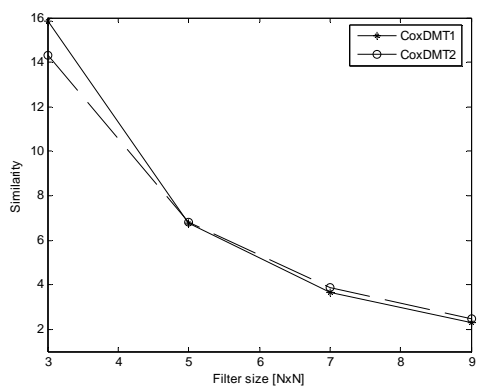


(a)

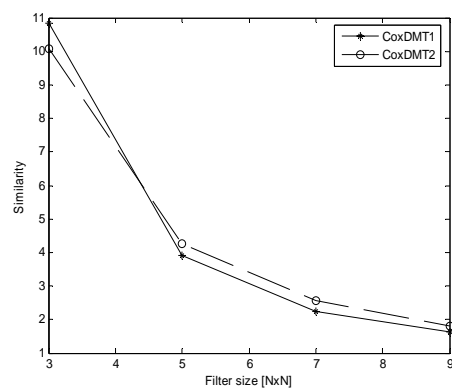


(b)

Figure 5.5 Similarity measurements of (a) Lena and (b) Baboon images under JPEG compression attack.



(a)



(b)

Figure 5.6 Similarities of watermarks under lowpass filtering using (a) Lena and (b) Baboon images.

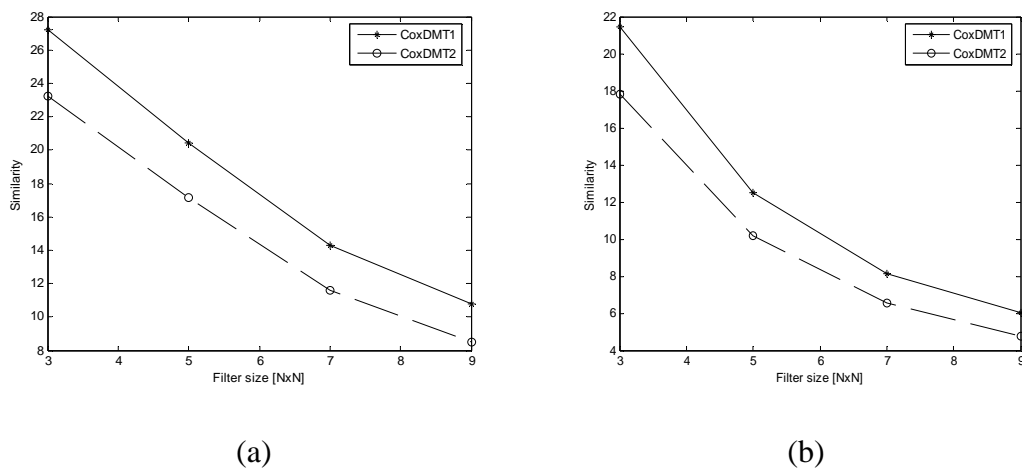


Figure 5.7 Similarities of watermarks under Wiener filtering using (a) Lena and (b) Baboon images.

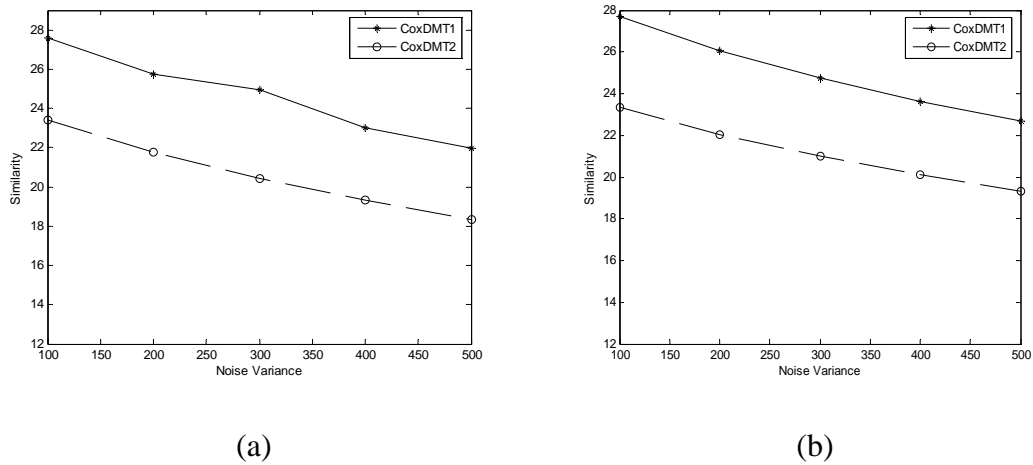


Figure 5.8 Similarities of watermarks under Gaussian noise addition using (a) Lena and (b) Baboon images.

5.3.2 Results of the public watermarking scheme

We investigate the effects of the recombining processes for the multiwavelet filter bank on the public watermarking scheme by performing the same watermark insertion and watermark detection as described in the Section 5.2.2. Similar to the previous case, the PSNR of the watermarked image was set to 43 dB. This was done by selecting the appropriate embedding strength using Newton's root-finding method. The parameters T_1 and T_2 were set to 40 and 50, respectively (typical values used by Dugad et al. (1998)) and the watermark signal to be embedded is the sequence of random numbers generated from a Gaussian distribution of zero mean and unit variance.

The results obtained from using recombining methods 1 and 2 are called DugadDMT1 and DugadDMT2, respectively. Since the correlation value in (5-5) follows standard Gaussian distribution, the probability of false watermark detection can be estimated as follows (Miller and Bloom, 1999):

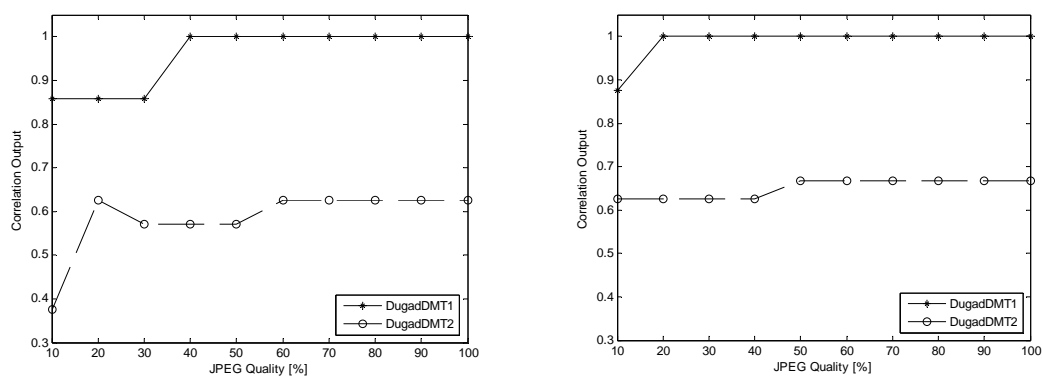
$$p = \frac{1}{\sqrt{2\pi}} \int_S^{\infty} e^{-\frac{1}{2}t^2} dt \quad (5-7)$$

In our simulations, the average value of threshold S is 7.21. This value yields a high reliability of the watermark detection scheme such that the probability of false alarm is less than 2.7978×10^{-13} . The performance of each watermarking scheme is measured to evaluate the robustness of the watermark.

To verify the robustness of the watermark, we first attack the watermarked image using JPEG compression with quality factors varying from 10% to 100%. The correlation output of the results using Lena and Baboon images are shown

in Figure 5.9(a) and Figure 5.9(b), respectively. We can see that the DugadDMT1 method gives more robust watermark.

Next, lowpass filtering and Wiener filtering were used to test the robustness of the watermarking schemes. As shown by the results in Figure 5.10 and Figure 5.11, the DugadDMT1 yields better results than the DugadDMT2. Finally, the robustness of the watermarking schemes was tested against adding Gaussian noise. As shown by the results in Figure 5.12, both schemes are robust against noise addition and the DugadDMT1 yields better results than the DugadDMT2. The experiment results clearly show that the recombining method 1 gives more robust watermark than method 2.



(a) (b)

Figure 5.9 Correlation output of (a) Lena and (b) Baboon images under JPEG compression attack.

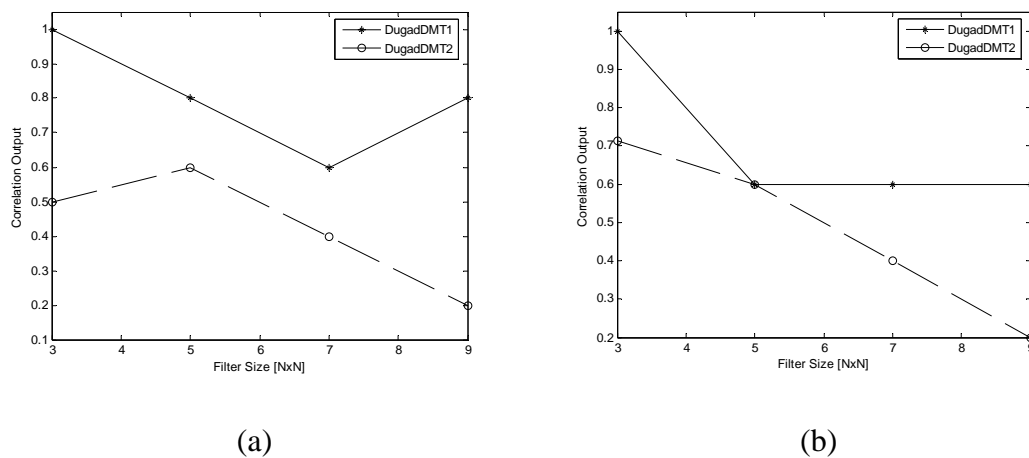


Figure 5.10 Correlation output of watermarks under lowpass filtering using
(a) Lena and (b) Baboon images.

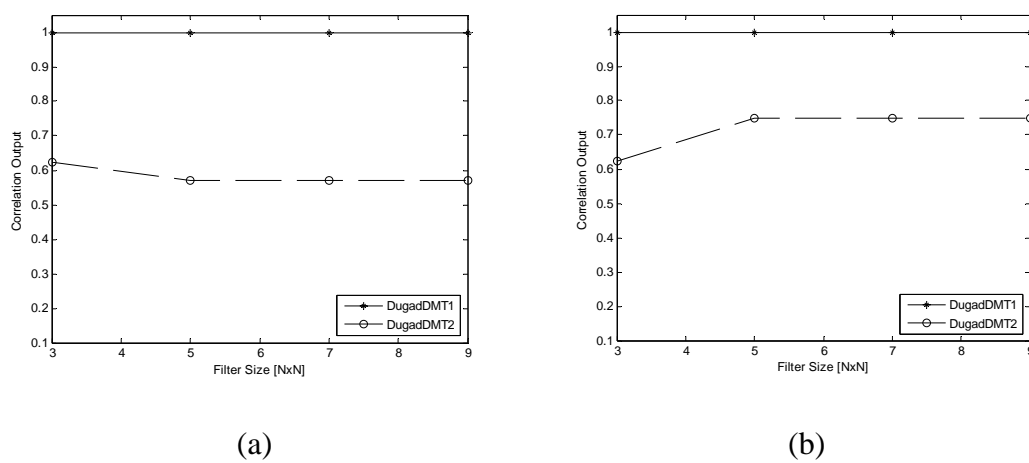


Figure 5.11 Correlation output of watermarks under Wiener filtering using
(a) Lena and (b) Baboon images.

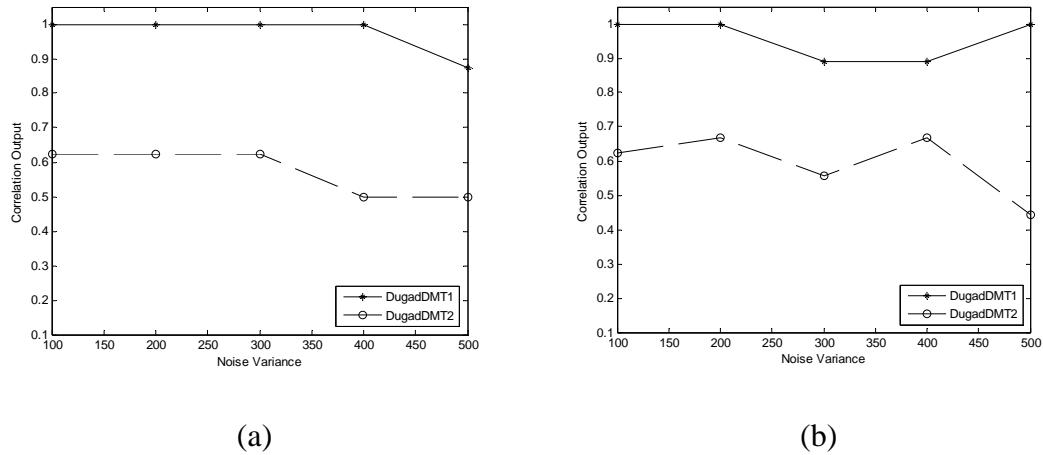


Figure 5.12 Correlation output of watermarks under Gaussian noise addition using
(a) Lena and (b) Baboon images.

5.4 Chapter Summary

From these simulations, we can see the effects of recombining processes for the multiwavelet filter bank on image watermarking in terms of robustness of the watermark. The results show that the watermarking method using the recombining method 1 gives more robust watermark than the one using method 2 for both private and public watermarking schemes. This is due to the fact that for the recombining method 1 which produces fewer subbands than method 2, the high-magnitude coefficients are likely to be in the same subbands. Thus, the algorithm using recombining method 1 is able to embed the watermark signal to more number of high-magnitude coefficients than the one using recombining method 2. Therefore, we selected the recombining method 1 for the development of our multiwavelet-based image watermarking scheme. In the next chapter, we will propose the performance improvement of image watermarking scheme using genetic algorithm.

CHAPTER VI

PERFORMANCE IMPROVEMENT OF IMAGE WATERMARKING SCHEME USING GENETIC ALGORITHMS

6.1 Introduction

In the previous chapter, the effects of the recombining processes for the multiwavelet filter bank on image watermarking from the view point of robustness of the watermark have been investigated. Then, the recombining method 1 has been selected for the development of multiwavelet-based image watermarking algorithm in this work since it gives more robust watermark than the one using method 2.

This chapter introduces an image watermarking algorithm based on the discrete multiwavelet transform and the genetic algorithm for the application of copyright protection. In this algorithm, the watermark is embedded to the discrete multiwavelet transform coefficients larger than some threshold values based on Dugad et al. (1998). In order to improve performance of watermarking algorithm, previous research works have concentrated on exploiting the characteristics of the human visual system in watermarking process (PodilChuk and Zeng, 1998; El-Khamy et al., 2002). In this work, the performance of watermarking scheme is improved by using an artificial intelligence techniques called genetic algorithms (GA). The GA is applied to search for optimal watermarking parameters in order to achieve performance improvement.

Finally, comparisons between the algorithms with and without GA are made. In addition, the results are compared with the ones from previous work.

6.1.1 Previous work

Several watermarking algorithms have been developed in the past. Dugad et al. (1998) proposed the spread spectrum image watermarking technique in the discrete wavelet transform (DWT) domain. They embed a watermark with a constant weighting factor into the perceptually significant coefficients in the high frequency subbands in order to preserve invisibility. However, it is not robust to common signal processing. Consequently, the development of a new algorithm that can satisfy both invisibility and robustness is needed.

Improvements in performance of watermarking schemes can be obtained by exploiting the characteristics of the human visual system (HVS) in watermarking process. It is possible to embed perceptually invisible watermarks with high energy in an image so that the watermark is robust (Langelaar et al., 2000). In 2002, El - Khamy et al. introduced a robust technique for image watermarking based on the concept of HVS and wavelet-based data fusion algorithms. Kwon and Tewfik (2002) proposed an adaptive image watermarking scheme in the multiwavelet transform domain using successive subband quantization and a perceptual modeling. Kwon et al. (2002) have extended the idea of Kwon and Tewfik (2002) by using a stochastic visual modeling. This model is based on a noise visibility function (NVF) that uses local image properties for watermark embedding.

Another way to improve the performance of watermarking schemes is to use artificial intelligence techniques. The image watermarking problem can be viewed as an unconstrained and multi-objective optimization problem. Therefore, it can be

solved by GA or any optimization tools. In the past, there have been a few references in application of GA to image watermarking problems. Huang and Wu (2000) proposed a watermarking method based on the DCT and GA. They embed the watermark with visually recognizable patterns into the image by selectively modifying the middle-frequency parts of the image. The GA is applied to search for the locations to embed the watermark in the DCT coefficient blocks such that the quality of the watermarked image is optimized. Shieh et al. (2004) presented a watermarking optimization technique similar to Huang and Wu (2000). They applied GA to find the optimum frequency bands for watermark embedding into DCT-based watermarking system which can simultaneously improve security, robustness and image quality of the watermarked image.

6.1.2 Contributions

The contributions of this chapter are as follows:

1. This chapter introduces the spread spectrum image watermarking algorithm using the discrete multiwavelet transforms. Performance improvement with respect to existing algorithms is obtained by GA optimization. The improved performance of a technique proposed in this chapter is demonstrated through simulation results.
2. A design of multi-objective function in the GA optimization of multiwavelet-based image watermarking scheme is proposed. Two factors related to invisibility and robustness and of a watermark are used for the objective function.
3. To the best of author's knowledge, this work is the first to propose a GA optimization of multiwavelet-based image watermarking scheme. It offers a

significant advantage by providing both high quality of the watermarked image and robust watermark.

This chapter is organized as follows: Watermarking in the discrete multiwavelet transform domain with GA optimization is described in Section 6.2. Section 6.3 discusses the experimental results. The conclusions of this study can be found in Section 6.4.

6.2 Proposed technique

This section elaborates on the proposed technique in details.

6.2.1 Multiwavelet-based image watermarking algorithm

In this chapter, a robust image watermarking algorithm in the discrete multiwavelet transform domain based on the method proposed by Dugad et al. (1998) with a slight modification is presented. The watermark insertion is performed in the DMT domain by applying the 3-level multiwavelet decomposition using the DGHM multiwavelet and optimal prefilters from Attakitmongcol et al. (2001). The recombining method for the multiwavelet filter bank is method 1. Since the approximation subband contains the high-energy components of the image, the watermark is not embedded in this subband to avoid visible degradation of watermarked image. Furthermore, the watermark is not embedded in the subbands of the finest scale due to the low-energy components to increase the robustness of the watermark. More details of this algorithm can be found in Section 5.2.2.

6.2.2 Improving watermarking performance by GA

To design a digital image watermarking system, there have always been three conflicting objectives occurred. These are visual quality, robustness, and the

amount of embedded information. This work employs the GA to search for suitable parameters in order to achieve the performance improvement of a digital image watermarking algorithm.

Performance of digital image watermarking algorithm can be improved in many ways. One might consider adjusting some parameters of the watermarking procedures to achieve a better performance. In this work, there are 3 parameters to be considered: embedding strength (α), embedding threshold (T_1) and detection threshold (T_2). These parameters are searched for each subband which is required to embed watermark. The searching objective function is designed by using two factors related to robustness and invisibility of a watermark. Hence, this can be considered as a multi-objective function. The diagram of proposed algorithm is shown in Figure 6.1 and details of GA are described as follows:

1) Chromosome Encoding: There are 30 chromosomes used in this work. The chromosomes are encoded using a binary string encoding scheme. Each chromosome represents 3 parameters to be searched with the resolution of 32 bits for each parameter, resulting in total length of 96 bits. The detection threshold T_2 must be strictly larger than the embedding threshold T_1 for the purpose of robustness in the watermark detection. This yields the relationship between T_1 and T_2 as follows:

$$T_2 = T_1 + T_d \quad (6-1)$$

where T_d is to be searched for the optimum value (instead of T_2). Consequently, each chromosome consists of α , T_1 and T_d .

2) Objective Function Evaluation: The objective function of GA uses the universal quality index (Wang and Bovik, 2002) which matches the HVS accurately as the output image quality index, and uses the difference (DIF) between correlation z and the threshold S as a watermark detection index. UQI is an imperceptibility measure, while DIF is a robustness measure. An objective value W can be computed by equation (6-2), which is

$$W = \delta_{UQI} \times (1 - UQI) + \delta_{DIF} \times DIF \quad (6-2)$$

where δ_{UQI} and δ_{DIF} are weighting factors of UQI and DIF , respectively. Each weighting factor represents how important each index is during the searching process of GA. For example, if both indices are equally important, both factors should be 0.5 (the relationship $\delta_{UQI} + \delta_{DIF} = 1.0$ must hold).

3) Selection, Genetic Operation, and Replacement: In this work, the ranking selection has been employed for the selection process of GA. The probabilities of crossover and mutation are chosen to be 0.7 and 0.005, respectively (as described in the next section). The best chromosomes are then partially replaced for each generation. The GA process is repeated until the most fittest chromosomes (or parameter α , T_1 and T_2) are optimally found.

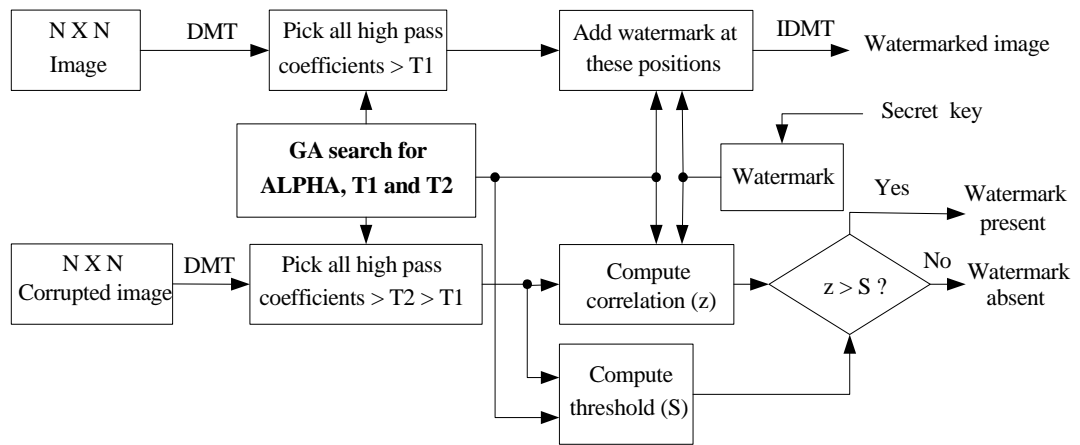


Figure 6.1 Improvement diagram for digital image watermarking using GA.

6.3 Results and Discussions

In this section, some experimental results are demonstrated to show the effectiveness of the proposed image watermarking scheme. In our watermark detection process, the original image is not required but the secret key and the resulting parameters from GA are needed. Therefore, the blindness of the watermarking scheme is partially lost. Thus, this becomes a semi-blind watermarking scheme. The invisibility and robustness of the watermark are tested by watermarking the original images with the resulting parameters from GA. The results obtained from the proposed method, called GADugadDMT1, are compared with the results of the DugadDMT1 method and Dugads method. In the DugadDMT1 method and Dugads method, the parameters α , T_1 and T_2 are set to 0.2, 40 and 50, respectively (a typical value used by Dugad et al. (1998)).

6.3.1 Results of performance improvement by GA

Even though the capability of GA for finding optimal solutions is widely accepted, some parameters of GA are chosen to be supervised in order to ensure that the resulting α , T_1 and T_2 are optimally found. In this section, there are three parameters of GA that are observed: probability of crossover, probability of mutation and number of chromosomes. These initial values of each GA parameter are randomly selected. After that, one parameter is varied while the others are fixed. Figures 6.2(a) – (b) display the results of α , T_1 and T_2 by varying the probability of crossover from 0.1 to 1.0. The results clearly show that the most suitable probability of crossover that gives the best (minimum) objective value is approximately 0.7. In the same manner, the results of varying the probability of mutation are shown in Figures 6.3(a) – (b) and the results of varying the number of chromosomes are illustrated in Figures 6.4(a) –

(b). These give the best probability of mutation approximately at 0.005 and the best number of chromosomes at 30. These three GA parameters are finally chosen for this work. Note that the objective values in Figures 6.2 – 6.4 are scaled in the clearer plots for comparison purpose.

Figures 6.5 – 6.10 illustrate the convergence of GA optimization by the example of the image subbands at 50 generations of the two images; Lena and Baboon. The resulting parameters, which are α , T_1 and T_2 from GA optimization of four test images, are shown in the Tables 6.1 – 6.4. These parameters are varied to achieve the most suitable for different characteristics.

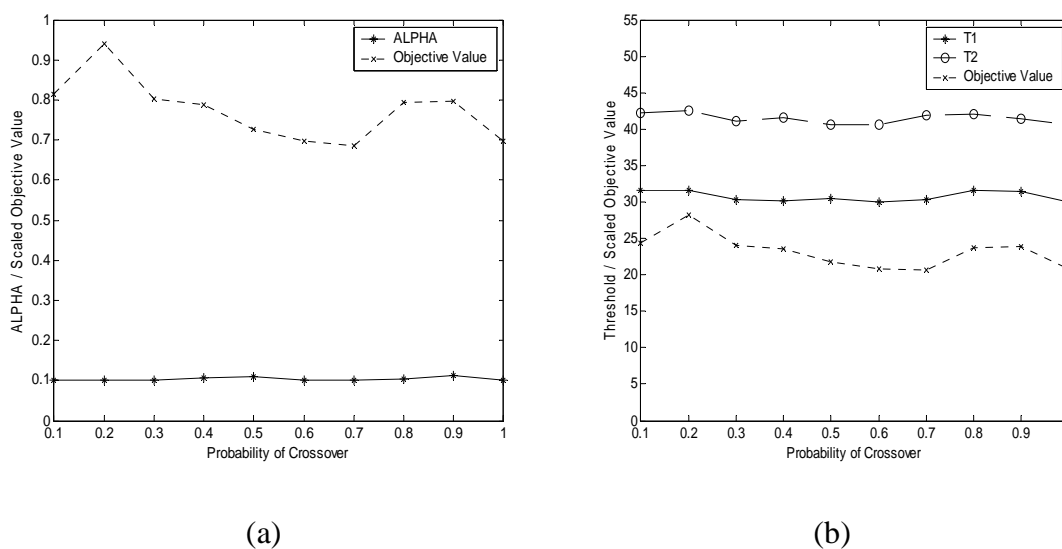
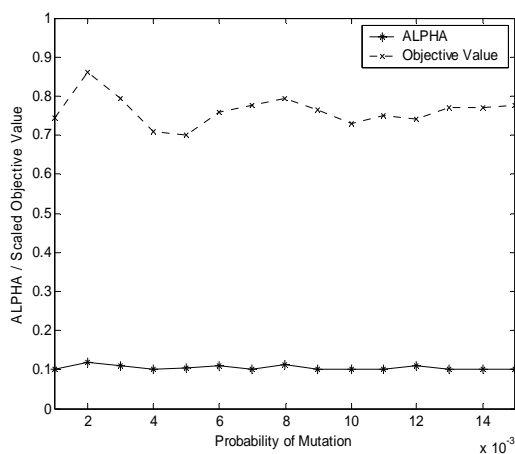
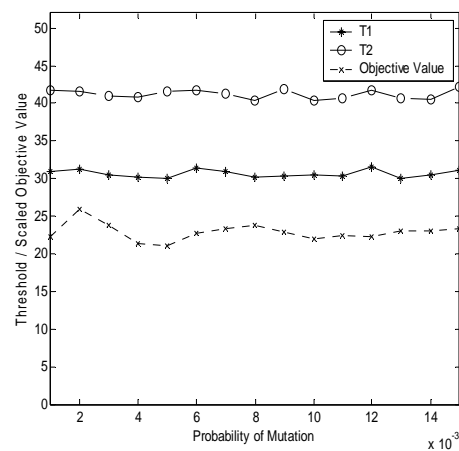


Figure 6.2 The results of ALPHA (α), T_1 , and T_2 for probability of crossover varying from 0.1 to 1.0.

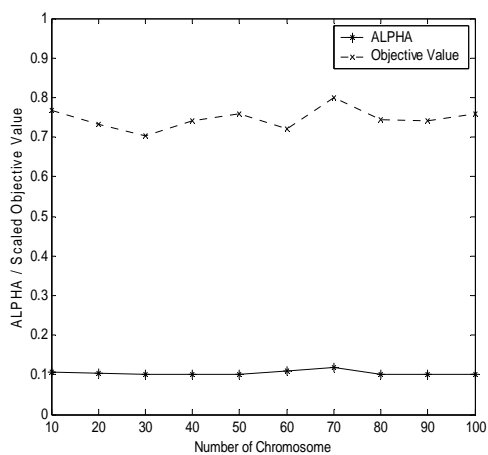


(a)

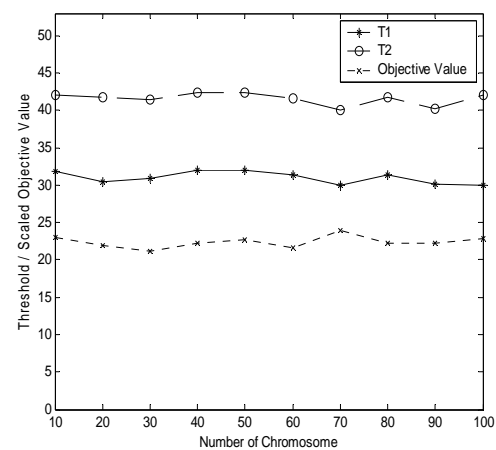


(b)

Figure 6.3 The results of ALPHA (α), T_1 , and T_2 for probability of mutation varying from 0.001 to 0.015.



(a)



(b)

Figure 6.4 The results of ALPHA (α), T_1 , and T_2 by varying the number of chromosomes from 10 to 100.

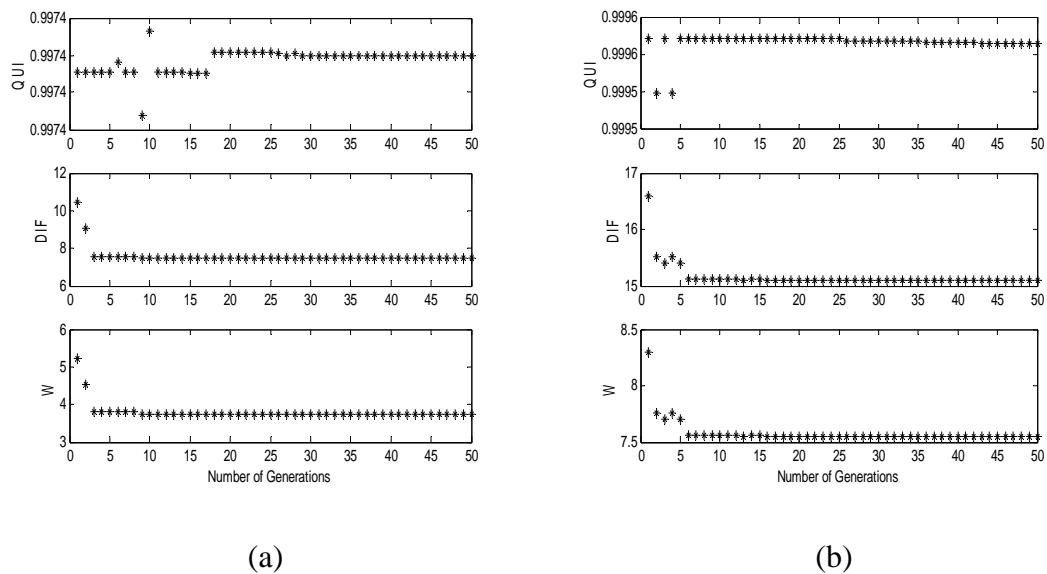


Figure 6.5 UQI , DIF and W from searching process of (a) LH_2 and (b) HL_2 subbands for Lena image.

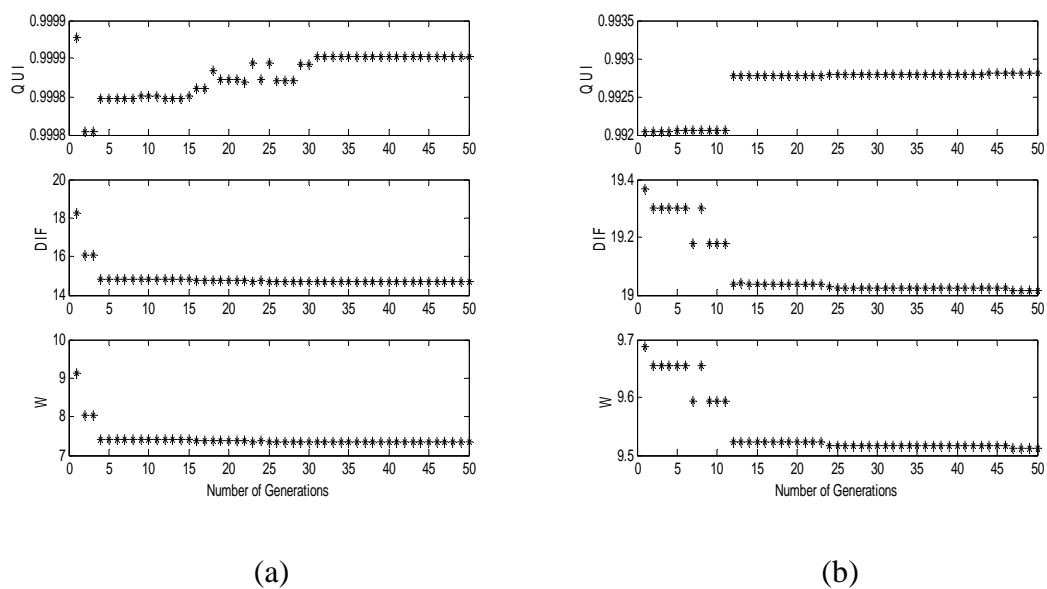
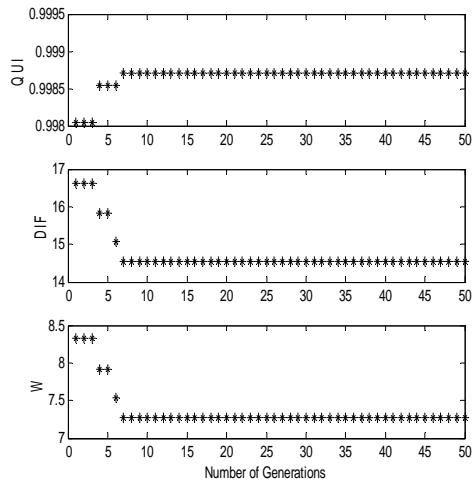
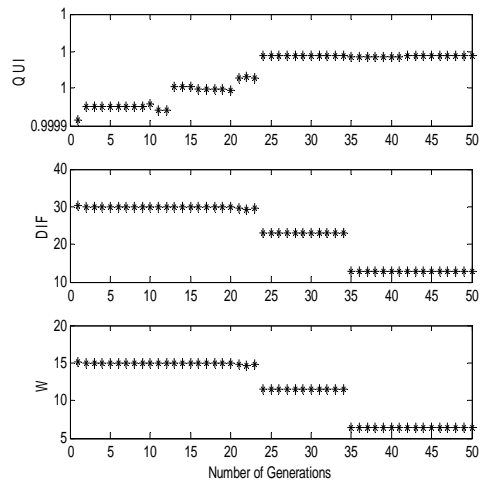


Figure 6.6 UQI , DIF and W from searching process of (a) HH_2 and (b) LH_3 subbands for Lena image.

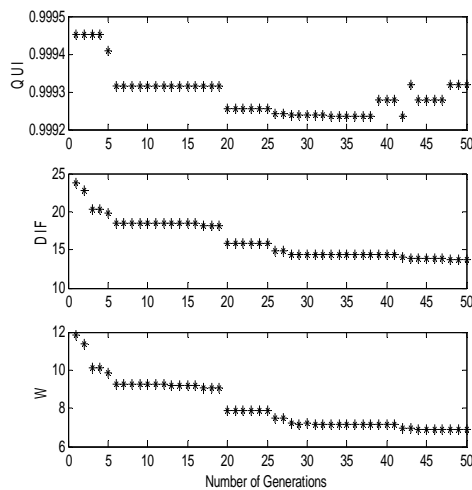


(a)

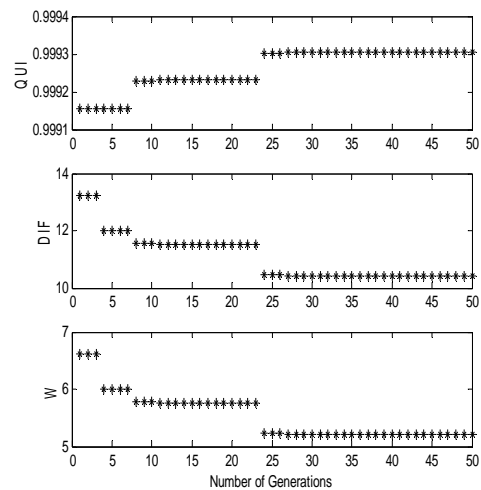


(b)

Figure 6.7 UQI , DIF and W from searching process of (a) HL_3 and (b) HH_3 subbands for Lena image.



(a)



(b)

Figure 6.8 UQI , DIF and W from searching process of (a) LH_2 and (b) HL_2 subbands for Baboon image.

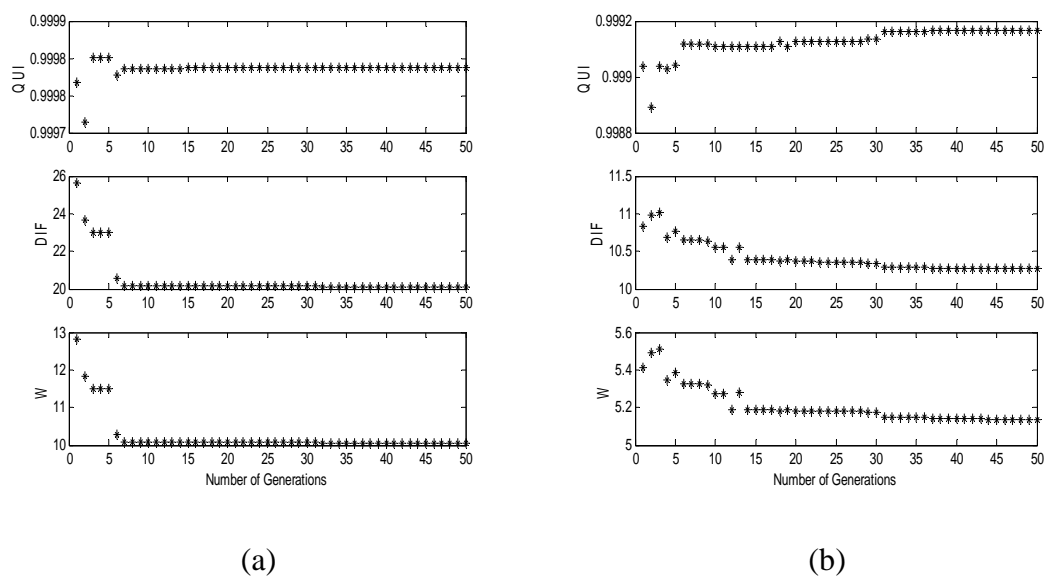


Figure 6.9 UQI , DIF and W from searching process of (a) HH_2 and (b) LH_3 subbands for Baboon image.

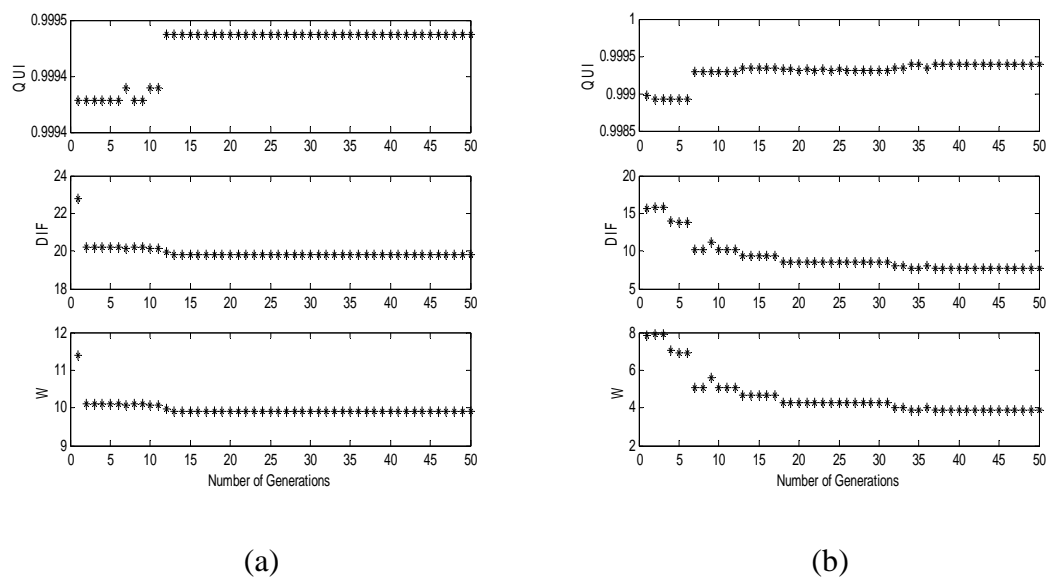


Figure 6.10 UQI , DIF and W from searching process of (a) HL_3 and (b) HH_3 subbands for Baboon image.

Table 6.1 Parameters α , T_1 and T_2 from GA search of the Lena image.

Subband	α	T_1	T_2
1. LH_2	0.10052	30.900	42.505
2. HL_2	0.10190	36.195	47.490
3. HH_2	0.10039	30.395	41.074
4. LH_3	0.10010	31.078	42.427
5. HL_3	0.10004	30.976	41.503
6. HH_3	0.20639	38.496	49.213

Table 6.2 Parameters α , T_1 and T_2 from GA search of the Baboon image.

Subband	α	T_1	T_2
1. LH_2	0.10791	30.020	40.104
2. HL_2	0.10013	30.422	40.522
3. HH_2	0.10057	31.340	41.931
4. LH_3	0.10030	30.463	40.498
5. HL_3	0.10029	30.317	41.516
6. HH_3	0.10009	30.976	41.386

Table 6.3 Parameters α , T_1 and T_2 from GA search of the Gold Hill image.

Subband	α	T_1	T_2
1. LH_2	0.10048	30.496	41.320
2. HL_2	0.10089	36.760	47.584
3. HH_2	0.10628	39.227	50.675
4. LH_3	0.10680	31.912	42.024
5. HL_3	0.10055	30.580	42.008
6. HH_3	0.10427	30.564	40.657

Table 6.4 Parameters α , T_1 and T_2 from GA search of the Pepper image.

Subband	α	T_1	T_2
1. LH_2	0.10065	30.938	41.584
2. HL_2	0.10241	30.354	40.664
3. HH_2	0.11037	30.053	40.090
4. LH_3	0.10501	31.704	44.768
5. HL_3	0.10010	30.231	40.329
6. HH_3	0.11938	39.647	50.871

6.3.2 Invisibility test results

The output image quality is tested by watermarking the original images with the resulting parameters from GA. Then, the PSNR and the UQI to are used compare the image quality between the original and the watermarked images. Figure 6.11 shows the watermarked version of the Lena image with PSNR 46.07 dB. From this figure, it is difficult to find any quality degradation in watermarked image. The results of watermarked image quality are shown in Table 6.5 and Table 6.6. It can be shown that the GADugadDMT1 method can improve the PSNR of the watermarked image about 5 dB when compared with Dugads method.



Figure 6.11 (a) Original Lena image and (b) watermarked image with PSNR 46.07 dB.

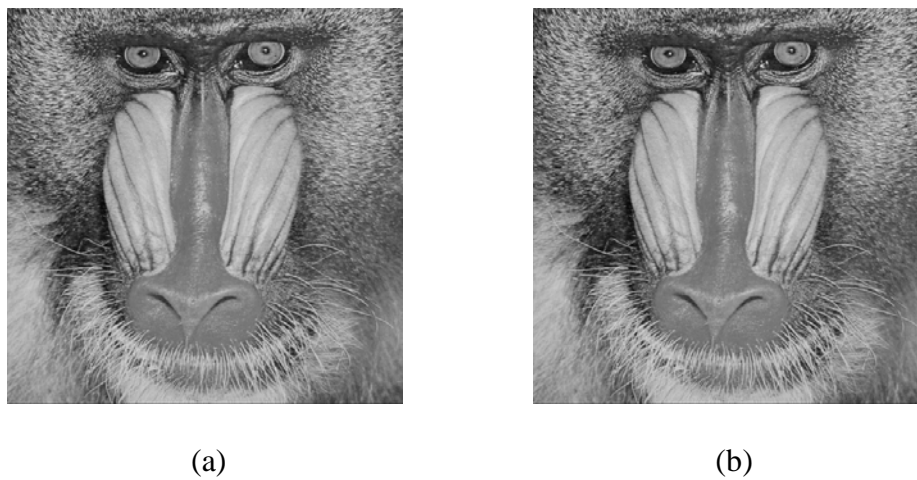


Figure 6.12 (a) Original Baboon image and (b) watermarked image with PSNR 41.87 dB.



Figure 6.13 (a) Original Gold Hill image and (b) watermarked image with PSNR 45.66 dB.



Figure 6.14 (a) Original Pepper image and (b) watermarked image with PSNR 44.48 dB.

Table 6.5 Comparison of PSNR between Dugads, DugadDMT1 and GADugadDMT1 methods.

Image	PSNR (dB)		
	Dugads	DugadDMT1	GADugadDMT1
Lena	41.33	41.18	46.07
Baboon	34.67	34.95	41.87
Gold Hill	40.40	39.77	45.66
Pepper	39.25	38.94	44.48

Table 6.6 Comparison of UQI between Dugads, DugadDMT1 and GADugadDMT1 methods.

Image	UQI		
	Dugads	DugadDMT1	GADugadDMT1
Lena	0.9681	0.9802	0.9917
Baboon	0.9868	0.9891	0.9972
Gold Hill	0.9666	0.9804	0.9937
Pepper	0.9638	0.9718	0.9896

6.3.3 Robustness test results

To investigate the robustness of the watermark, the watermarked image is attacked using JPEG compression, lowpass filtering, Wiener filtering, Gaussian noise addition, image cropping and image rotation. Then, the watermark detection process is performed and the correlation output is computed. The examples of different types of attacks to the watermarked image are shown in Figure 6.15. Firstly, lossy compression to the watermarked image is performed. Figure 6.16 verifies the robustness of the watermark when the watermarked image is attacked by JPEG compression. Figure 6.16(a) shows the detector response of 6 subbands of the Lena image under JPEG compression with quality factor 10% and Figure 6.16(b) shows the detector response of the extracted watermark during detection process of subband LH_2 . Figure 6.17 shows the correlation output when the watermarked images (Lena and Baboon) are compressed with various JPEG qualities from 10 to 100%. The results clearly show that GADugadDMT1 yields better results than Dugads method.



(a)



(b)



(c)



(d)



(e)



(f)

Figure 6.15 Different type of attacks to watermarked image (a) JPEG compression (quality factor 10%), (b) lowpass filtering (9×9), (c) Wiener filtering (9×9), (d) Gaussian noise addition (variance 500), (e) cropping 50 % of its surrounding and (f) image rotation (1.0° clockwise).

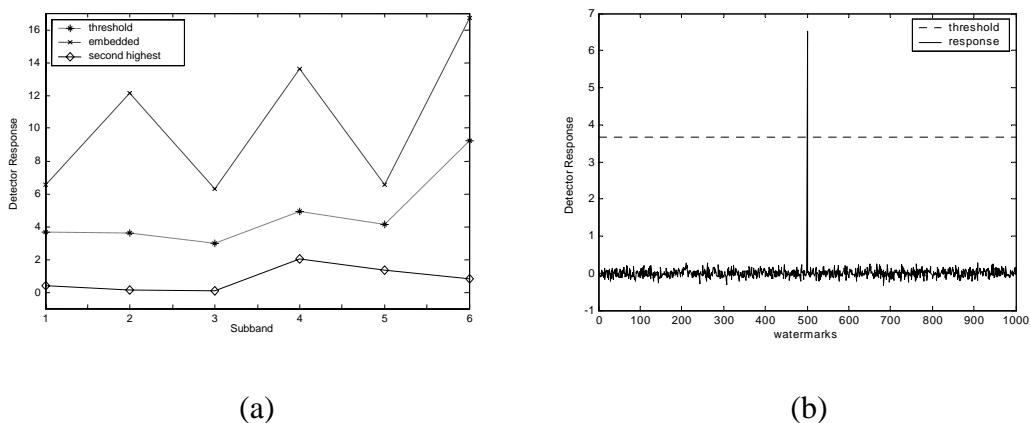


Figure 6.16 JPEG compression attack (quality factor 10%). (a) Detector response of 6 subbands. (b) Detector response of the extracted watermark of subband LH_2 when 1,000 watermarks were tested.

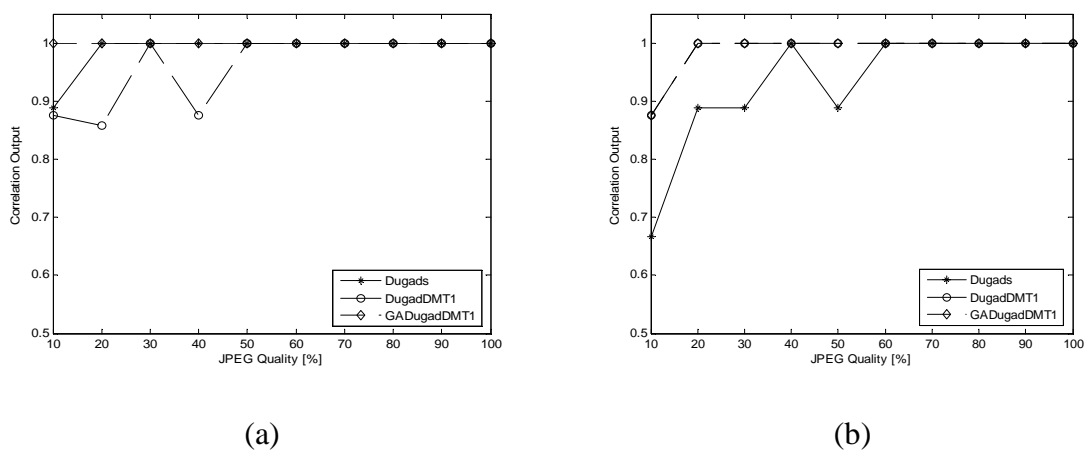


Figure 6.17 Correlation output using JPEG compression with various qualities of (a) Lena image and (b) Baboon image.

Image filtering is also performed to the watermarked image such as lowpass filtering and Wiener filtering. Figure 6.18 and Figure 6.19 show the correlation output when the watermarked images are attacked by lowpass filtering and Wiener filtering, respectively. The results show that GADugadDMT1 gives better results than Dugads method.

Noise addition is another method to verify the robustness of the watermark. In many cases, the degradation and distortion of the image come from noise addition. In our experiment, Gaussian noise of mean 0 and variance varying from 200 to 500 is added to the watermarked images and watermark detection is performed. It can be seen from Figure 6.20 that the GADugadDMT1 yields the most robust watermark to Gaussian noise addition in this study.

The next image manipulation is cropping. The watermarked images are attacked by cropping 10%, 20%, 30%, 40% and 50% of its surroundings. The results in Figure 6.21 show that GADugadDMT1 gives the most robust watermark.

Rotation is an important kind of geometric transformation. After applying geometric transformations to the watermarked image, most watermarking detectors are unable to detect the embedded watermark because the synchronization between the extracted watermark and the embedded watermark is lost. Figure 6.22 shows the results of the robustness test by image rotation. Bilinear interpolation is used to perform the rotation of watermarked images. The rotation angle varies from 0.2° to 1.0° clockwise. After rotation, four corners of the rotated image are cropped in order to keep the size of the rotated image the same as the original one. The results show that our proposed method and Dugads method have little resistance to this kind of attack.

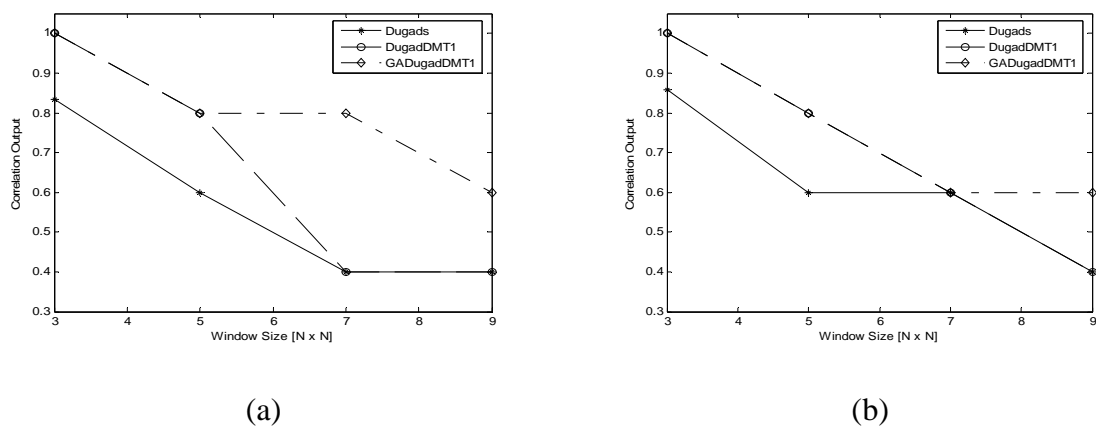


Figure 6.18 Correlation output using lowpass filtering with various sizes of window filters of (a) Lena image and (b) Baboon image.

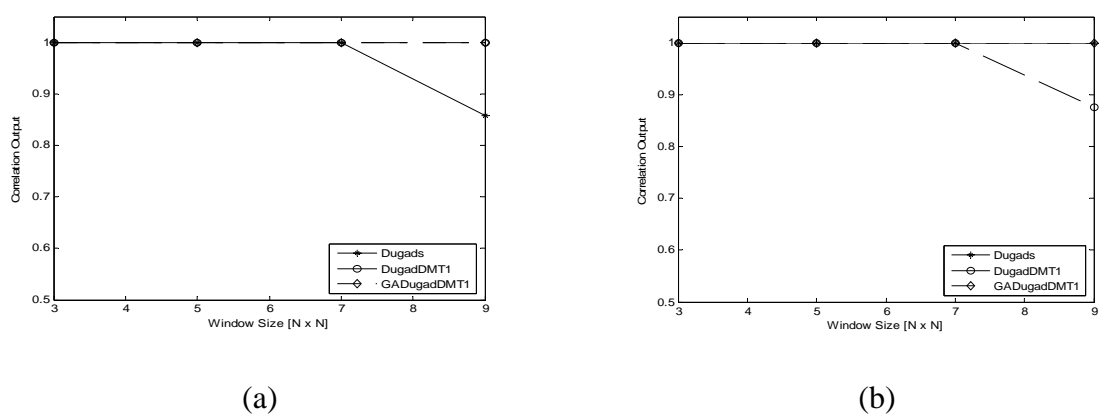
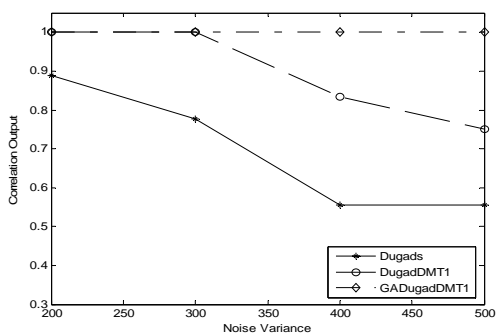
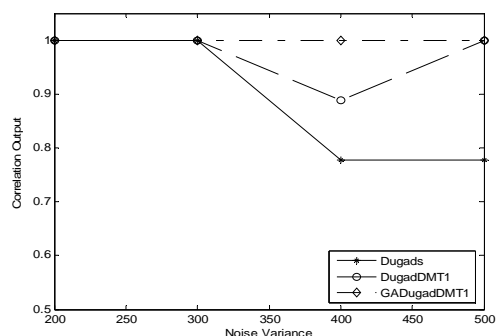


Figure 6.19 Correlation output using Wiener filtering with various sizes of window filters of (a) Lena image and (b) Baboon image.

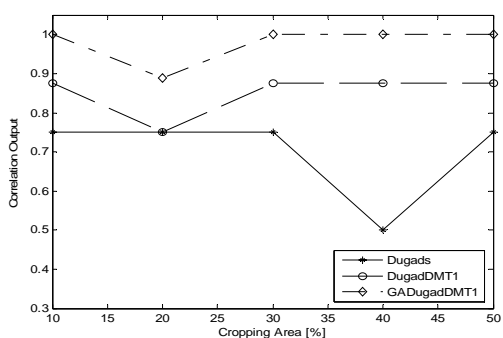


(a)

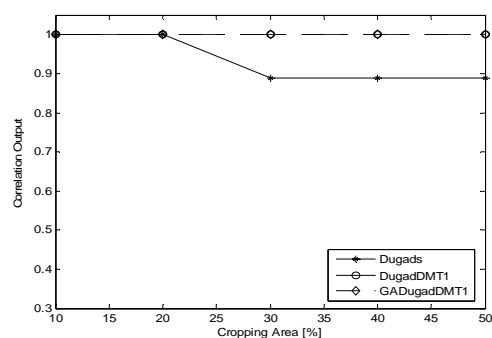


(b)

Figure 6.20 Correlation output using Gaussian noise addition with various noise variances of (a) Lena image and (b) Baboon image.



(a)



(b)

Figure 6.21 Correlation output using cropping with various cropping areas of (a) Lena image and (b) Baboon image.

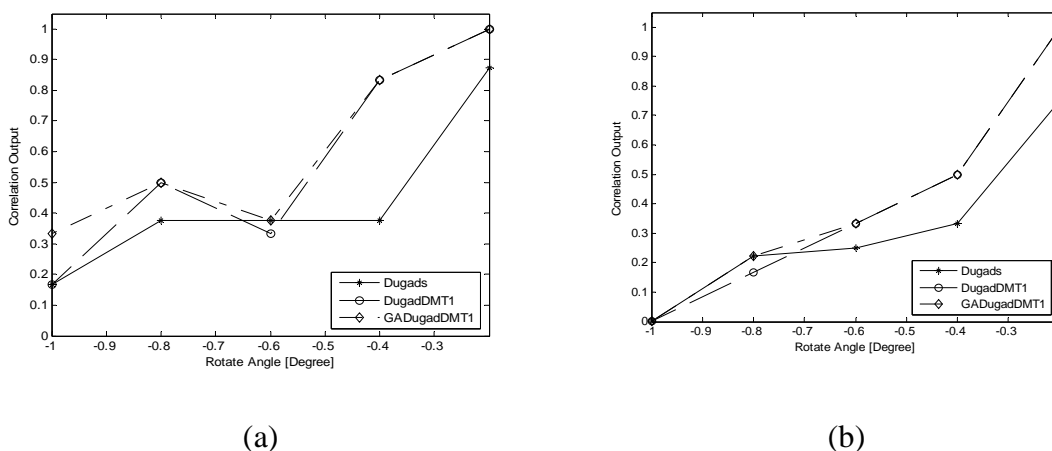


Figure 6.22 Correlation output using rotation with various rotation angles of
(a) Lena image and (b) Baboon image.

6.4 Chapter Summary

In this chapter, the image watermarking algorithm using the discrete multiwavelet transform has been proposed. Performance improvement with respect to the existing algorithms is obtained by GA optimization. In the improvement process, GA is used to search for suitable values of threshold values and the embedding strength. These parameters are optimally varied to achieve the most desirable ones for original images with different characteristics. The key characteristics used in the multi-objective searching process are the universal quality index, the difference between correlation z and the threshold S . The experimental results show that the proposed method can improve the quality of the watermarked image and give watermark which is more robust than what achieved by the previous works.

CHAPTER VII

A NOVEL ROBUST IMAGE WATERMARKING TECHNIQUE BASED ON MULTIWAVELET TRANSFORM

7.1 Introduction

In the previous chapter, we have proposed a new approach for optimization in image watermarking by using GA. The watermark is a sequence of randomly generated real numbers which can only be detected by employing the detection theory. In this chapter, we attempt to develop image watermarking algorithms which are portable to a variety of applications such as copyright protection, fingerprinting and identification. Therefore, we require that the watermark be binary and be not only detectable but also extractable. The embedding technique is based on the parent-child structure of the multiwavelet transform called “triple tree” and this technique does not require the original image in the watermark extraction. By use of Neyman-Pearson criterion in the detection process, a decision threshold is explicitly derived without referring to the original image. Invisibility and robustness are used as the performance measures. The peak signal to noise ratio (PSNR) is used as an objective measure of the invisibility while the normalized correlation coefficient and bit error rate are used to measure the robustness.

7.1.1 Previous work

Digital watermarking offers a means for protecting intellectual property of digital multimedia contents that have been explosively exchanged in the digital world. This technique is based on embedding information data (called watermark) into the digital contents. The main requirements of digital watermarking are invisibility, robustness and data capacity. These requirements are mutually conflicting, and thus, in the design of a watermarking system, the trade off has to be made (Langelaar et al., 2000).

In recent years, some multiwavelet-based image watermarking algorithms have been proposed. Kwon and Tewfik (2002) proposed an adaptive image watermarking scheme in the discrete multiwavelet transform (DMT) domain using successive subband quantization and a perceptual modeling. The watermark was Gaussian random sequence with unit variance and the original image was needed for watermark detection. In 2002, Zhang et al. proposed a novel watermarking scheme for an image, in which a logo watermark was embedded into the multiwavelet domain of image using back-propagation neural network (BPN). Due to the learning and adaptive capabilities of BPN, their scheme provides good robustness. In 2004, Kumsawat et al. proposed an image watermarking algorithm using the DMT. The GA was applied to search for optimal watermarking parameters to improve the quality of the watermarked image and the robustness of the watermark. Wang and Lin (2004) proposed a wavelet-tree quantization for copyright protection watermarking. The wavelet coefficients were grouped into a predefined structure called supertree. Watermark bits were embedded by quantizing supertree and the resulting difference between quantized and unquantized trees were used later be used for watermark extraction.

In our proposed algorithm, the watermark is embedded into the DMT coefficients using multiwavelet tree technique. The proposed watermarking technique is resistant against various attacks as will be demonstrated in the examples. Finally, we compare our experimental results with the results of the previous works.

7.1.2 Contributions

The contributions of this chapter are as follows:

1. The development of multiwavelet tree called “triple tree” from the parent-child dependencies of multiwavelet hierarchical subband decomposition for our image watermarking algorithm.

2. The design of a novel robust image watermarking using triple tree.

The remainder of this chapter is organized as follows. In Section 7.2, the preliminaries of multiwavelet tree are introduced. Watermarking in the multiwavelet transform domain is described in Section 7.3. Section 7.4 discusses the experimental results. The conclusions of our study can be found in Section 7.5.

7.2 Multiwavelet Tree

In recent years, multiwavelet transformation has gained a lot of attention in signal processing applications. The main motivation of using multiwavelet is that it is possible to construct multiwavelets that simultaneously possess desirable properties such as orthogonality, symmetry and compact support with a given approximation order. These properties are not possible in any scalar wavelet. Figure 7.1(a) shows a four-level multiwavelet decomposition using the DGHM multiwavelet with optimal orthogonal prefilter (Attakitmongkol et al., 2001).

Multiwavelet transform coefficients have the property that the related coefficients in different scales are located at the same orientation and location in the

multiwavelet hierarchical decomposition. With the exception of the highest frequency subbands, every coefficient at a given scale can be related to a set of coefficients at the next finer scale of similar orientation. The coefficient at the coarse scale is called the parent, and all coefficients corresponding to the same spatial location at the next finer scale of similar orientation are called children. For the multiwavelet hierarchical subband decomposition, the parent-child dependencies are shown in Figure 7.1(b). For a given parent, the set of all coefficients at all finer scales of similar orientation corresponding to the same location are called descendants. A multiwavelet-tree that descends from a single coefficient in the subband HL_4 is also shown in Figure 7.1(b).

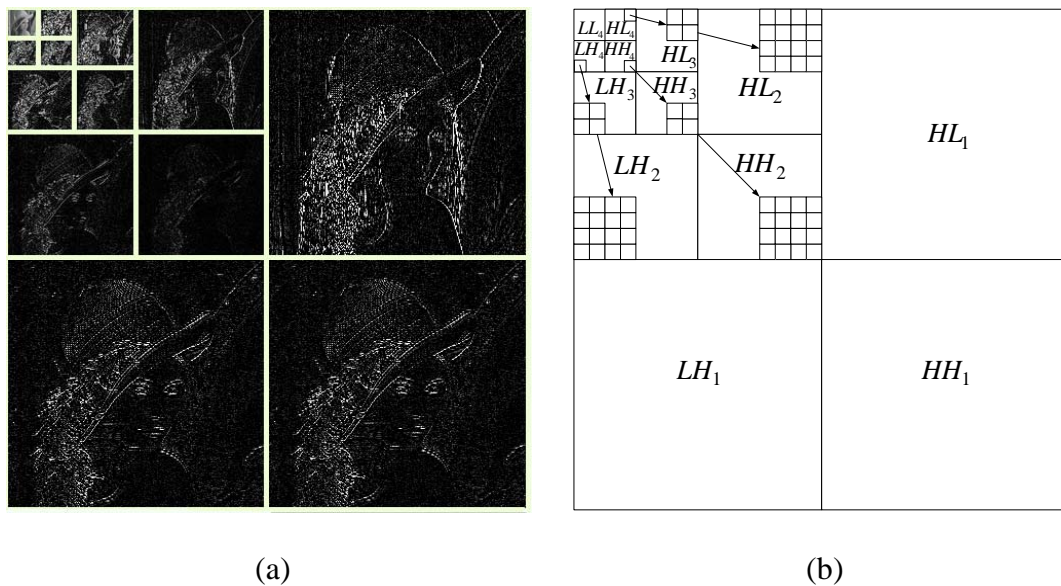


Figure 7.1 (a) Four-level multiwavelet decomposition of image having size of 512×512 pixels and (b) the parent-child dependencies of multiwavelet-tree.

Without significant loss of generality, we shall focus on watermarking still images with 256 gray levels of size 512×512 pixels. To trade off between the invisibility and robustness of the watermark, the high-energy subband (LL_4) is not used. Furthermore, the coefficients in highest frequency subbands (LH_1 , HL_1 and HH_1) are not used since they often contain little energy.

In other subbands, we group the coefficients corresponding to the same spatial location together. Figure 7.2(a) shows an example of a group with one coefficient from HL_4 , 4 coefficients from HL_3 , and 16 coefficients from HL_2 . The coefficients of the same group correspond to various frequency bands of the same spatial location and the same orientation. The total number of groups is equal to the number of coefficients in LH_4 , HL_4 and HH_4 , each of which has 32×32 coefficients. There are a total of $3 \times 32 \times 32 = 3072$ groups. We denote each group of multiwavelet tree by Tg_m , where $m = 1, 2, \dots, 3072$.

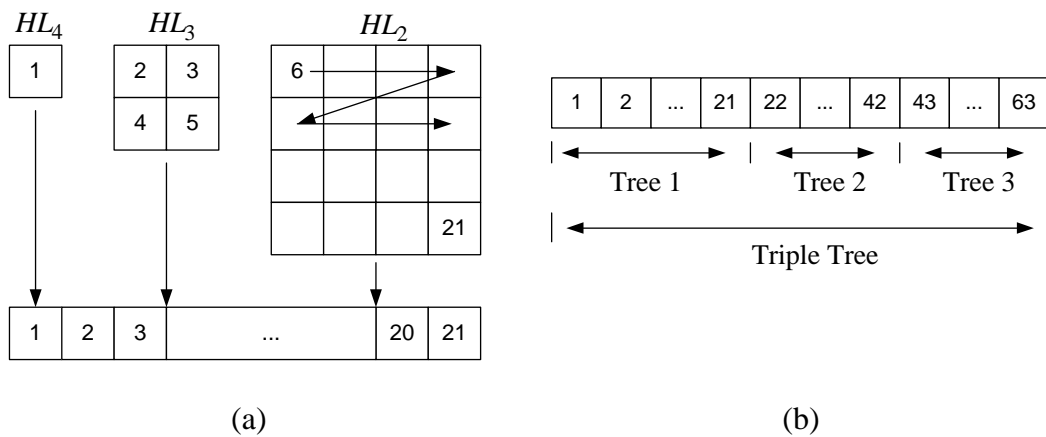


Figure 7.2 (a) A group of multiwavelet coefficients in each tree and (b) an example of triple tree.

7.3 Proposed Technique

In this section, we first give a brief overview of the watermark embedding and watermark extracting processes in the DMT domain based on the concept of multiwavelet tree. We then describe the detection analysis of our proposed method.

7.3.1 Watermark embedding algorithm

The watermark embedding algorithm is as follows:

1. Generate a random watermark W using a secret key, where W is a binary sequence of watermark bits, and $W = \{w_i\}$ for $i = 1, 2, \dots, N_w$, where N_w is the length of watermark. This sequence is produced from a real value uniform pseudo random number generator by setting the binary sequence to -1 when the real value sequence smaller than 0.5 and to 1 when the generator output is greater than or equal to 0.5. The watermark sequence can be generated by mapping a meaningful signature or text through a certified one-way deterministic function or hash function (Zeng and Liu, 1999).

2. Transform the original image into four-level decomposition using the DMT. Then, we create multiwavelet-trees from multiwavelet coefficients and rearrange them into 3072 groups.

3. Define JPEG quantization matrix (William and Joan, 1993) by $Q = [q_{ab}], \{a, b = 1, \dots, 8\}$. We quantize each group of multiwavelet tree Tg_m by using JPEG quantization matrix in order to gain the robustness to JPEG compression attack. The standard JPEG quantization table is shown in Figure 7.3. The quantized multiwavelet tree Tq_m are given by

$$Tq_m = \left\lceil \frac{Tg_m}{Q} \right\rceil \quad (7-1)$$

where $\lceil \cdot \rceil$ designates rounding to the nearest integer.

4. For increasing the watermarking security, order the groups Tq_m in a pseudorandom manner. The random numbers can be generated using the secret key. We further combine the coefficients of every three groups together to form “a triple tree: Tt_n ”, for $n = 1, 2, \dots, 1024$. Each watermark bit is embedded into one triple tree. An example of a triple tree is illustrated in Figure 7.2(b).

5. For watermark embedding, select N_w triple trees (Tt_i for $i = 1, 2, \dots, N_w$). Then, modify the coefficients in triple trees in the watermark embedding process as follows:

$$Ttw_i = \begin{cases} Tt_i + Tt_i \bmod 2 - 1 & \text{if } w_i = 1 \\ Tt_i - Tt_i \bmod 2 & \text{otherwise} \end{cases} \quad (7-2)$$

where Ttw_i is a triple tree that contains watermark information and mod is the modulo operator.

6. Perform inverse quantization to each group of all triple trees and pass the modified DMT coefficients through the inverse DMT to obtain the watermarked image. The inverse quantization of multiwavelet-tree Tiq_m is given by

$$Tiq_m = \lceil Tq_m \times Q \rceil \quad (7-3)$$

The watermark embedding process and flow chart of the proposed watermark embedding algorithm are shown in Figure 7.4 and Figure 7.5, respectively.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Figure 7.3 JPEG quantization matrix.

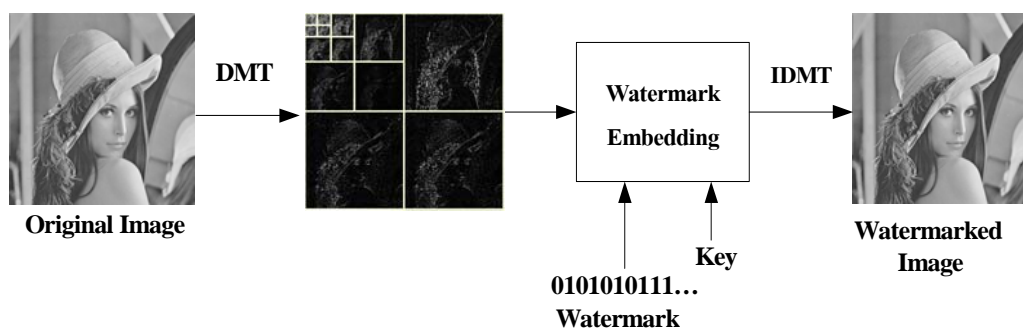


Figure 7.4 Watermark embedding process.

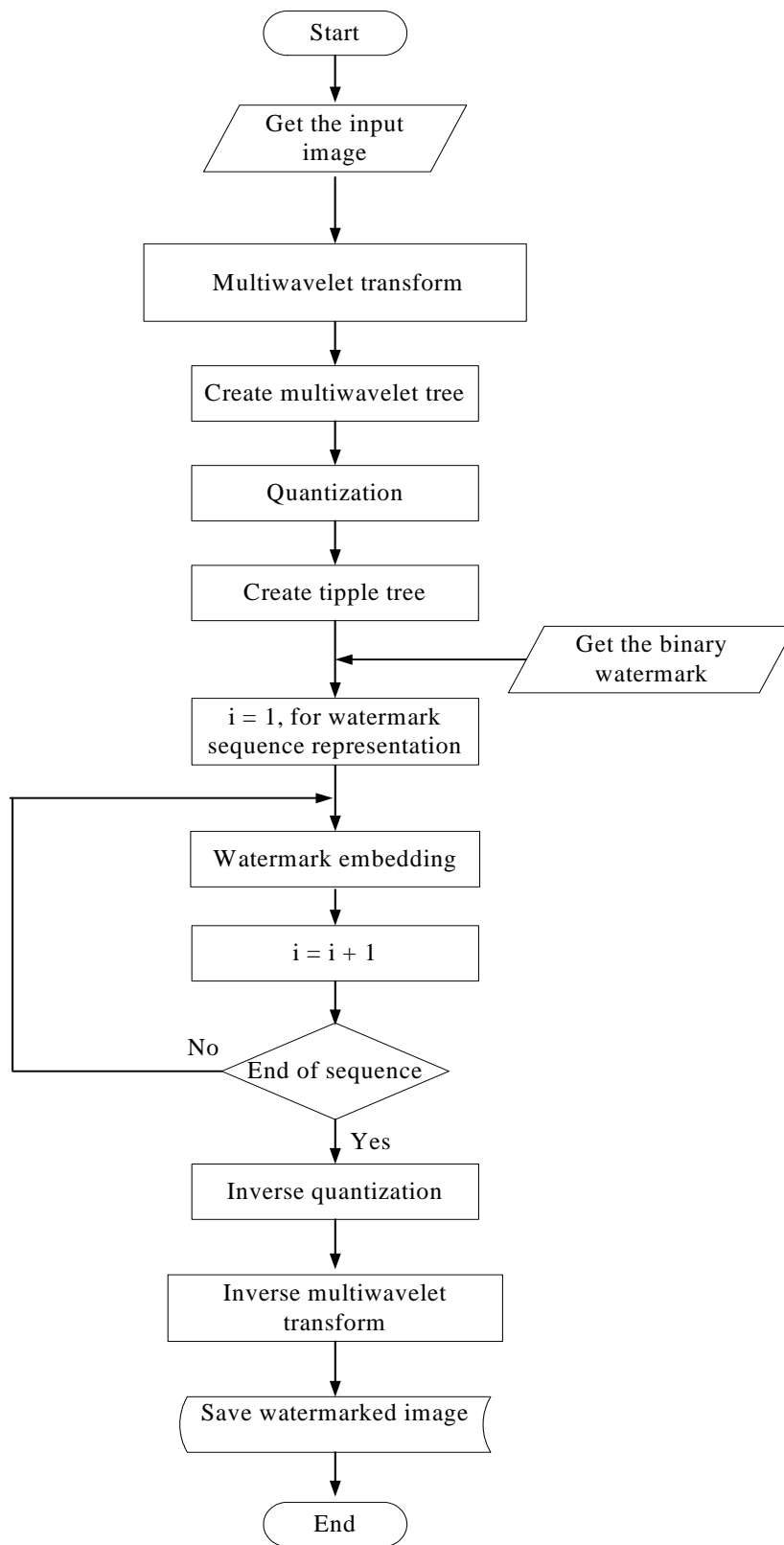


Figure 7.5 Flow chart of the proposed watermark embedding algorithm.

7.3.2 Watermark extracting algorithm

1. Transform the watermarked image into four level decomposition using the DMT. Then, create the multiwavelet-trees and rearrange them into 3072 groups.

2. Apply JPEG quantization matrix to each group of multiwavelet tree. Then, order the groups in a pseudorandom manner using the same secret key. We further combine every 3 groups to form a triple tree Tt_n , for $n = 1, 2, \dots, 1024$.

3. To extract the embedded watermark, select the same N_w triple trees Tt_i from all triple trees and count the *even* and *odd* coefficients in each triple tree based on $Tt_i \bmod 2$ computation. The embedded bit can now be recovered from a triple tree as follows:

$$\tilde{w}_i = \begin{cases} 1 & \text{if } odd \geq even \\ -1 & \text{otherwise} \end{cases} \quad (7-4)$$

4. After extracting the watermark, use normalized correlation coefficients to quantify the correlation between the original watermark and the extracted one. A normalized correlation between W and \tilde{W} is defined as (Wang and Lin, 2004):

$$\rho(W, \tilde{W}) = \frac{\sum_{i=1}^{N_w} w_i \tilde{w}_i}{\sqrt{\sum_{i=1}^{N_w} w_i^2 \sum_i \tilde{w}_i^2}} \quad (7-5)$$

where W and \tilde{W} denote original watermark and extracted one, respectively. If the correlation $\rho(W, \tilde{W})$ is greater than the pre-specified threshold T , the watermark has been detected. The watermark extracting process and a flow chart of the proposed watermark extracting algorithm are shown in Figure 7.6 and Figure 7.7, respectively.

7.3.3 Watermark detection analysis

For application of copyright protection, the watermark detection aims to verify whether a given watermark is embedded in the suspected image or not. Thus, the detection of a watermark is formulated as a binary hypothesis testing problem as follows:

H_0 : The suspected image does not contain the watermark, or it contains a different watermark which is not the one under investigation.

H_1 : The suspected image contains the watermark.

For a given threshold T , the system performance can be measured in terms of the probability of false alarm $P_{fa}(T)$ (i.e., the probability to detect a watermark in an image that is not watermarked or, is watermarked with a different watermark) and the probability of false rejection $P_{fr}(T)$ (i.e., the probability of failure to detect an existing watermark). $P_{fa}(T)$ and $P_{fr}(T)$ can be expressed as

$$P_{fa}(T) = \text{Prob} \{ \rho(W, \tilde{W}) \geq T \mid H_0 \} \quad (7-6)$$

and

$$P_{fr}(T) = \text{Prob} \{ \rho(W, \tilde{W}) < T \mid H_1 \} \quad (7-7)$$

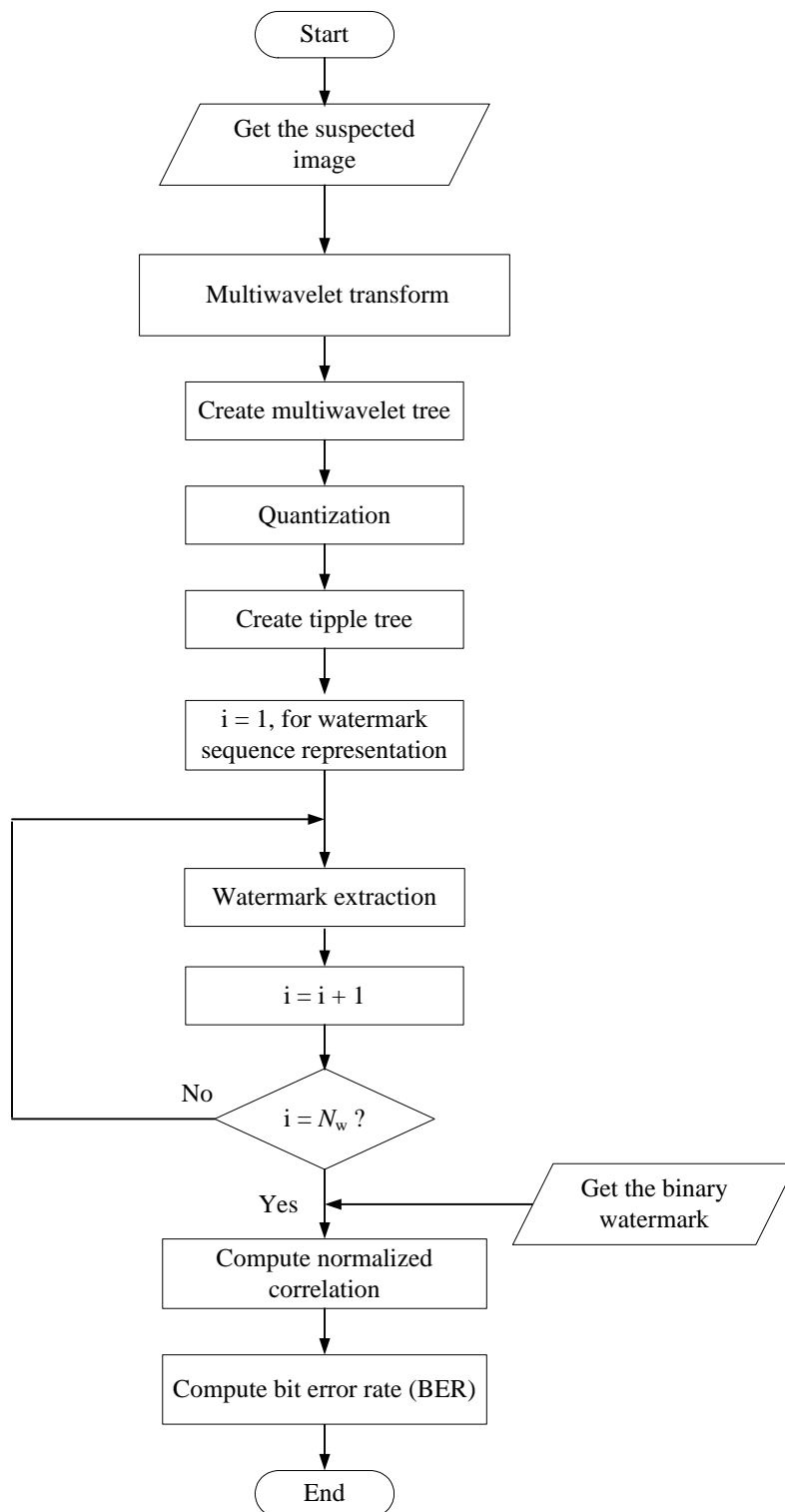


Figure 7.6 Flow chart of the proposed watermark extracting algorithm.

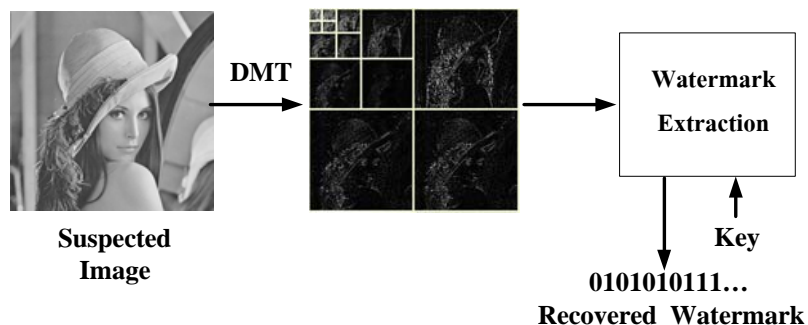


Figure 7.7 Watermark extracting process.

where $\text{Prob}\{A|B\}$ is the probability of event A given event B . Depending on the application, these two types of error probabilities might have different significance. For copyright protection application, it is very important to have low or zero false alarm rates. (Typically, the false alarm rate is kept at a small level in the order of 10^{-12} to 10^{-6} (Hippenstiel, 2002).)

In order to decide the valid hypothesis, the correlation $\rho(W, \tilde{W})$ is compared with threshold T . The Neyman-Pearson criterion can be used to obtain threshold T in such a way that the false rejection probability is minimized for a fixed false alarm probability (Barni et al., 2001). The final step for watermark detection for the binary hypothesis case is:

If $\rho(W, \tilde{W}) \geq T$, watermark W is detected.

If $\rho(W, \tilde{W}) < T$, watermark W is not detected.

From Equation (7-3), the normalized correlation coefficient is bounded by ± 1 as $-1 \leq \rho(W, \tilde{W}) \leq 1$. Since the watermark is a binary sequence of ± 1 , we have

$$\sum_{i=1}^{N_w} w_i^2 = \sum_{i=1}^{N_w} (\tilde{w}_i)^2 = N_w \quad (7-8)$$

Let P_E be the probability of bit error during extraction and be defined as $P_E = \text{Prob}(w_m \neq \tilde{w}_m)$. If we let $b_i = w_i \tilde{w}_i$, for $m = 1, 2, \dots, N_w$, then $b_i = -1$ indicates a bit error and $b_i = 1$ indicates no error. The normalized correlation coefficient can also be written as

$$\rho(W, \tilde{W}) = \frac{\sum w_i \tilde{w}_i}{N_w} = \frac{\sum b_i}{N_w} \quad (7-9)$$

and

$$P_{fa}(T) = \text{Prob} \{ \sum b_i \geq N_w T \mid H_0 \} \quad (7-10)$$

Then, the probability of false alarm can be computed by (Kundur, 1999; Hippenstiel, 2002)

$$P_{fa} = \sum_{k=((T+1)/2)N_w}^{N_w} \binom{N_w}{k} P_E^{N_w-k} (1-P_E)^k \quad (7-11)$$

where $\binom{N_w}{k} = \frac{N_w!}{k!(N_w-k)!}$. The false alarm probability depends on P_E , N_w and T .

In the case that the image is not a watermarked copy, it is reasonable to assume $P_E = 0.5$. Then,

$$P_{fa} = \sum_{k=((T+1)/2)N_w}^{N_w} \binom{N_w}{k} (0.5)^{N_w} \quad (7-12)$$

We choose the threshold $T = 0.4$ that has an associated probability of false alarm less than 2.02×10^{-20} for a 512 bit watermark.

7.4 Results and Discussions

In this section, some experimental results are demonstrated to show the effectiveness of the proposed image watermarking scheme. First, the image visual quality after watermark embedding is investigated. Then, we evaluate the robustness of the watermark under common signal processing and image compression. Finally, we compare our experimental results with the results of the previous work. The well-known wavelet-tree quantization for copyright protection watermarking by Wang and Lin (2004) has been used for comparison. The details of this algorithm can be found in Appendix D.

The experiments have been conducted by using the DGHM multiwavelet to decompose the original image. The test images are 256 gray-level images of size 512×512 pixels. A 512-bit binary watermark is generated randomly and used throughout the experiments.

7.4.1 Invisibility test results

We use the peak signal to noise ratio (PSNR) to measure the image quality of the watermarked image. The PSNR values of the watermarked images are 38.37 and 38.04 dB for Lena and Baboon, respectively. Figures 7.8(b) and 7.9(b) show the watermarked version of the Lena and Baboon images using the proposed technique, respectively. It can be seen that both watermarked images are not perceptually different from the original ones.



Figure 7.8 (a) Original “Lena” image and (b) watermarked image from the proposed method.

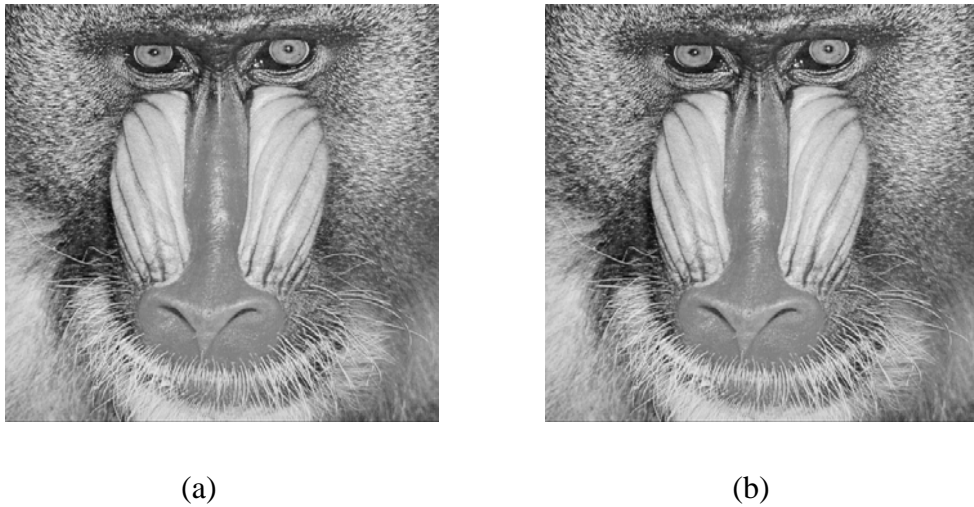


Figure 7.9 (a) Original “Baboon” image and (b) watermarked image from the proposed method.

7.4.2 Robustness test results

In order to measure the robustness and detection capability of our technique, the watermarked images are attacked by common signal processing and image compression, i.e. cropping, median filtering, Gaussian filtering, image rotations, JPEG, JPEG2000 and SPIHT compression. Then, we perform the watermark extraction process and compute the normalized correlation coefficient between original and extracted watermarks. In verification phase, the normalized correlation coefficient is compared with a threshold T to determine the existence of a watermark. The threshold T should be chosen to give a relatively small false alarm probability. For a 512-bit watermark, we list the false alarm probability for various thresholds in Table 7.1. We choose the threshold $T = 0.4$ which has an associated probability of false alarm less than 2.02×10^{-20} .

Since our system is a multi-bit watermarking, the bit error rate (BER) is a very useful measure of performance (Langelaar et al., 2000). The bit error rate is calculated as the number of incorrectly decoded bits divided by the total number of embedded bits in the watermarked image.

We first examine the robustness against JPEG compression. Figure 7.10(a) shows the normalized correlation coefficient for the watermarked image compressed by JPEG for compression ratio 5 to 30 using Lena and Baboon images. The BER values of watermark sequence corresponding to different compression ratios using JPEG compressions are shown in Figure 7.10(b). The watermark could be extracted from JPEG compression with compression ratio as high as 30. This demonstrates that the proposed scheme is very robust to JPEG compression.

JPEG2000 is a new image coding system that uses state-of-the-art compression technique based on wavelet technology (JPEG2000 our new standard, online, 2006). Its architecture should lend itself to a wide range of uses from portable digital cameras to advanced pre-press, medical imaging and other key sectors, such as mobile communication and digital library. It is expected that the JPEG2000 standard will become a popular image-coding standard in the coming future. Thus, we test the robustness with respect to JPEG2000 compression. Figure 7.11 shows the plot of normalized correlation coefficient and BER versus different compression ratios of JPEG2000 compression using Lena and Baboon images. In this case, the detector behaves significantly better than in the JPEG case. This could be explained by the fact that the image quality obtained by JPEG2000 is higher than the one obtained by JPEG at the same compression ratio. Therefore, the watermark signal is better preserved by JPEG2000.

Furthermore, we evaluate the robustness against cropping. We use a part of the image by selecting 10% to 50% of the original size at the center and cropping every other pixels. The results in Figure 7.12 show that the watermarks can survive very well.

Recent research in transform-based image compression has focused on the wavelet transform due to its superior performance over other transforms. The embedded zerotree wavelet (EZW) coding proposed by Shapiro (1993) makes a breakthrough in image coding which not only effectively removes the spatial redundancy across multiresolution scales but also provides fine scalability. The set partitioning in hierarchical trees (SPIHT) coding proposed by Said and Pearlman (1996) is one of the simplest and most efficient improvement of the EZW coding. The SPIHT-based method has therefore become the core technology of the emerging multimedia standards MPEG-4 (Mpeg industrial forum, online, 2005) and JPEG2000.

Finally, we examine the robustness against SPIHT wavelet compression, median filtering, Gaussian filtering and image rotations. The results obtained from our proposed method which is called DMT-Tree are compared with the method proposed by Wang and Lin (2004), which is called Method 1. For a fair comparison, the invisibility of the watermarked Lena image (PSNR around 38 dB) and embedding capacity (watermark 512 bits) for both schemes must be the same. The comparison results are listed in Table 7.2 to Table 7.4. According to these results, the normalized correlation coefficients of the extracted watermarks using our proposed method are always higher than the ones using Method 1. The results show that our proposed method yields significantly more robust watermark than the Method 1, except for the case when JPEG quality is 90. In this case, both methods produce the same robust watermark.

Table 7.1 False alarm probability for different thresholds.

Threshold value	False alarm rate
0.1	0.0121
0.2	2.4758×10^{-6}
0.3	4.7930×10^{-12}
0.4	2.0218×10^{-20}
0.5	4.9739×10^{-31}
0.6	4.6565×10^{-45}
0.7	1.0927×10^{-62}
0.8	6.1165×10^{-84}

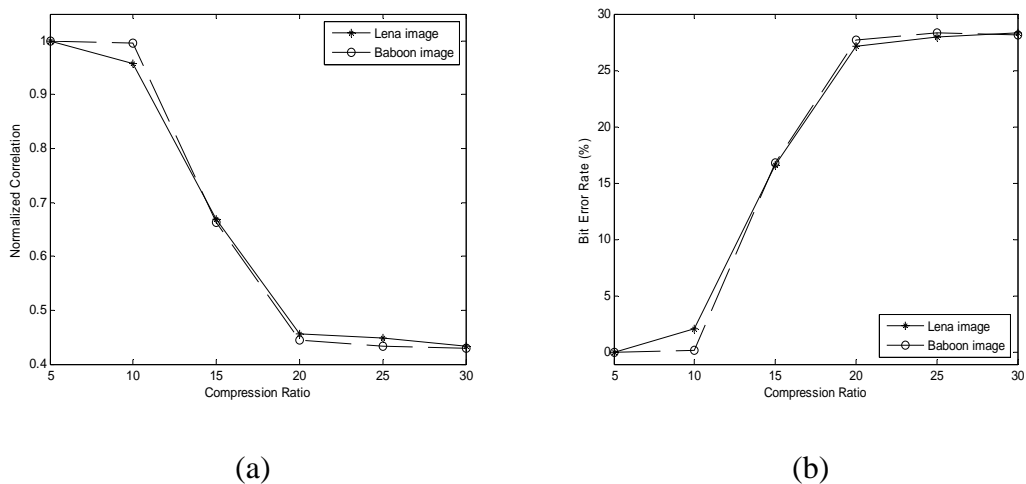


Figure 7.10 Plots of (a) Normalized correlation coefficient and (b) BER versus different compression ratios of JPEG compression using Lena and Baboon images.

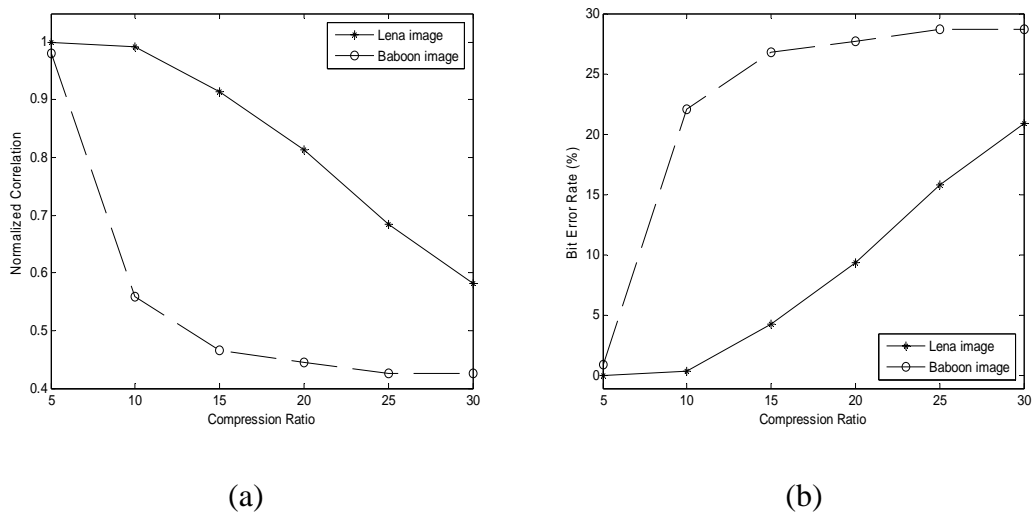


Figure 7.11 Plots of (a) Normalized correlation coefficient and (b) BER versus different compression ratios of JPEG2000 compression using Lena and Baboon images.

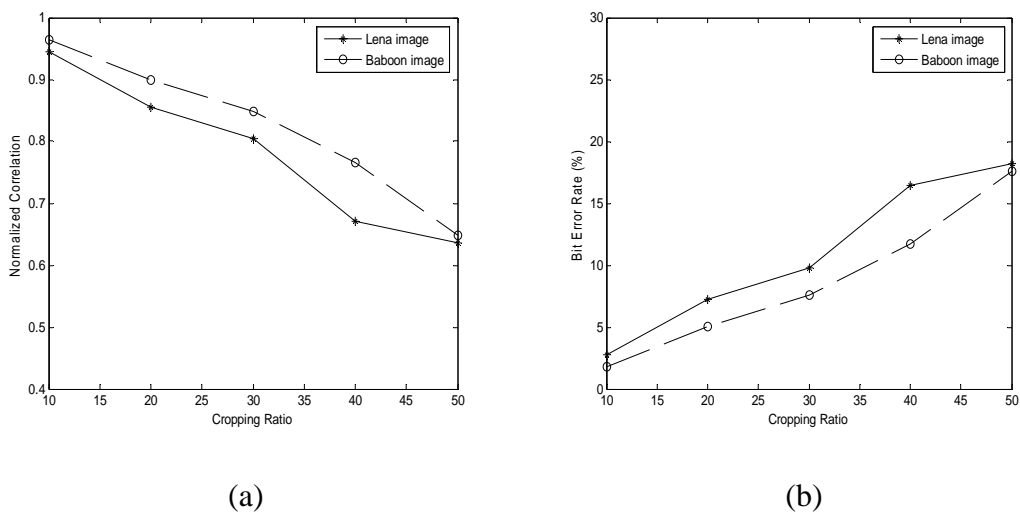


Figure 7.12 Plots of (a) Normalized correlation coefficient and (b) BER versus different cropping ratios of cropping attack using Lena and Baboon images.

Table 7.2 Normalized correlation using JPEG compression.

JPEG Quality factor (%)	Normalized Correlation	
	DMT-Tree	Method 1
30	0.5391	0.1500
40	0.7227	0.2300
50	0.9023	0.2600
70	0.9844	0.5700
90	1.0000	1.0000

Table 7.3 Normalized correlation using SPIHT compression.

Bit rate (bit per pixel)	Normalized Correlation	
	DMT-Tree	Method 1
0.3	0.5703	0.2100
0.4	0.7813	0.4100
0.5	0.9102	0.8500
0.6	0.9453	0.8300
0.7	0.9570	0.8500

Table 7.4 Normalized correlation using image processing attacks.

Attack	Normalized Correlation	
	DMT-Tree	Method 1
2x2 Median filtering	0.4648	0.3800
3x3 Median filtering	0.6445	0.5100
4x4 Median filtering	0.4492	0.2300
3x3 Gaussian filtering	0.6680	0.6400
Rotation 0.25	0.6484	0.3700
Rotation 0.5	0.4570	0.2900
Rotation 0.75	0.4375	0.2600
Rotation 1.0	0.4219	0.2400
Rotation -0.25	0.6523	0.3200
Rotation -0.5	0.4609	0.2300
Rotation -0.75	0.4375	0.2400
Rotation -1.0	0.4180	0.1600

From these experiments, the watermark using proposed watermarking technique is significantly more robust than the one using Method 1. This is due the predefined structure of multiwavelet tree called “triple tree” of the proposed algorithm. In creation of a triple tree, the multiwavelet tree is randomly selected using a secret key. The watermark bits spread over all groups of multiwavelet trees. As a result, the algorithm gains good robustness against watermark attacks. In addition, the proposed technique utilizes the quantization-based embedding strategy. Each multiwavelet tree is quantized using JPEG quantization matrix before creating a triple tree. This

quantization can be considered as pre-quantization for JPEG compression. Therefore, the embedded watermark will have fewer effects from quantization process in JPEG compression attack. Hence, the proposed algorithm gains the watermark robustness to JPEG compression attack.

7.5 Chapter Summary

This chapter proposed a new digital watermarking algorithm in the multiwavelet transform domain. The embedding technique is based on the parent-child structure of the transform coefficient called “triple tree”. By use of Neyman-Pearson criterion, a decision threshold is explicitly derived without referring to the original image. The experimental results show that the proposed watermarking technique is significantly more robust than Method 1. This is due to the predefined structure of multiwavelet tree called “triple tree” of the proposed algorithm. The watermark bits spread over all groups of multiwavelet trees. As a result, the watermark is robust against watermark attacks. In addition, the proposed technique utilizes the quantization-based embedding strategy. Hence, it gains the watermark robustness to JPEG compression attack.

CHAPTER VIII

COMPARATIVE PERFORMANCE OF MULTIWAVELET-BASED IMAGE WATERMARKING SCHEMES

8.1 Introduction

This chapter presents the performance comparisons of two image watermarking schemes in the multiwavelet transform domain. The first one is based on the concept of the multiwavelet-tree watermarking technique that has been designed in the previous chapter and the second one is based on the code division multiple access (CDMA) technique. The embedding information is a visually recognizable pattern which can be not only detectable but also extractable. Both techniques do not require the original image in the watermark extraction process. The normalized correlation and bit error rate are used to evaluate the robustness of the watermark and the evaluation process is performed on the watermarked images under the same image quality.

8.1.1 Previous works

In previous research, Fridrich and Golja (1999) presented a methodology for comparing the robustness of spread spectrum image watermarking techniques in the discrete cosine transform domain. Furthermore, the authors describe a methodology for converting a detectable, one bit watermark into a readable watermark and vice versa. Kurugollu et al. (2003) have compared four different wavelet

transforms including scalar wavelet, multiwavelet, complex wavelet and wavelet packet transforms, for the use in fusion based watermarking applications. The main aim of the paper was to evaluate the performance of these transforms in term of the robustness of the watermark under certain imperceptibility. Wang and Lin (2004) proposed a wavelet-tree quantization for copyright protection watermarking. The wavelet coefficients are grouped into a predefined structure called supertree. Watermark bits are embedded by quantizing supertree and the resulting difference between quantized and unquantized trees will later be used for watermark extraction.

In 2005, Kumsawat et al. proposed a new approach for optimization in wavelet-based image watermarking using genetic algorithm (GA). The watermark insertion and watermark extraction are based on the CDMA techniques and the watermark extraction process does not require the original image. Genetic algorithm is applied to search for optimal strength of the watermark in order to improve quality of the watermarked image and robustness of the watermark.

In this chapter, we focus our discussion on the comparison of robustness for multiwavelet-based image watermarking using two different embedding techniques. The first one is based on multiwavelet-tree technique. The other one is based on CDMA technique from Kumsawat et al. (2005) without applying GA process.

This chapter is organized into four sections. The next section describes the details of the multiwavelet-based image watermarking scheme. In Section 8.3, the experimental results and discussions are given. Section 8.4 presents conclusions of our study.

8.2 Multiwavelet-Based Image Watermarking Scheme

In this section, we first give a brief overview of the watermark embedding and watermark extracting in the DMT domain based on the concept of multiwavelet-tree. We then describe the CDMA watermarking technique in multiwavelet-based image watermarking scheme.

8.2.1 Multiwavelet-tree watermarking technique

We propose a robust image watermarking algorithm using the discrete multiwavelet transform which has been described in Chapter 7. The embedding technique is based on the parent-child structure of the multiwavelet transform called “triple tree” and does not require the original image in the watermark extraction.

8.2.1.1 Watermark embedding algorithm

To increase security, a pseudo-random permutation is performed first in order to disperse the spatial relationship of the binary watermark pattern. Therefore, it would be difficult for a pirate to detect or remove the watermark. We use W and W^* to denote the original watermark image and the permuted watermark image, respectively. The relationship between W and W^* can be expressed as $W^*(i, j) = W(i', j')$, where (i', j') is permuted to the pixel position (i, j) in a secret order.

To embed the watermark, the original image is first decomposed into four-levels using DMT. The watermark is then embedded into the DMT coefficients using multiwavelet-tree watermarking algorithm. The details of this algorithm can be found in Chapter 7. The watermark embedding process is shown in Figure 8.1.

8.2.1.2 Watermark extracting algorithm

To extract the embedded watermark, we transform the watermarked image into four-level decomposition using the DMT. The embedded bit can be recovered from DMT coefficients using multiwavelet-tree watermarking algorithm. Then, we perform inverse permutation of the recovered watermark \tilde{W}^* to obtain the extracted watermark \tilde{W} .

In our proposed method, the extracted watermark is a visually recognizable image. After extracting the watermark, we used normalized correlation coefficients to quantify the correlation between the original watermark and the extracted one. A normalized correlation between W and \tilde{W} is defined in Equation (7-5). For the application of copyright protection, a given watermark is detected if the correlation of the extracted watermark with the given watermark is above a pre-specified threshold. The watermark extracting process is shown in Figure 8.2.

8.2.2 CDMA watermarking technique

The CDMA watermarking technique is based on the proposed method in Kumsawat et al. (2005) and will be referred to as DMT-CDMA. For a fair comparison, we do not apply any intelligent technique to this watermarking algorithm. Next, we give a brief overview of this technique. The details of this CDMA watermarking technique can be found in the given reference.

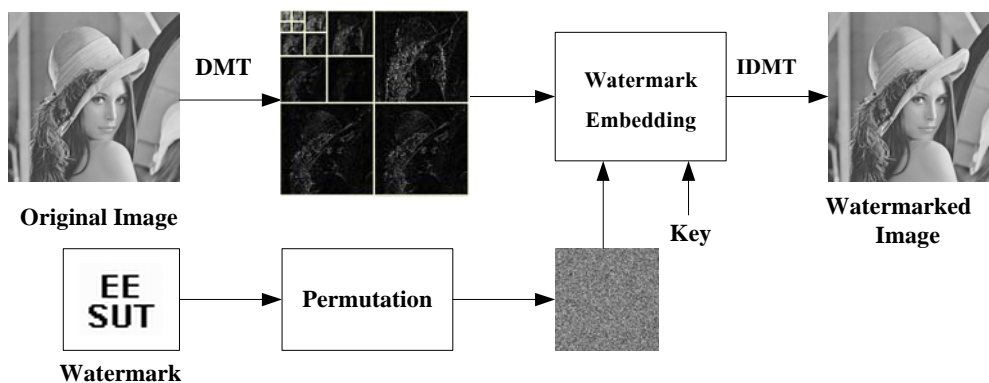


Figure 8.1 Watermark embedding process.

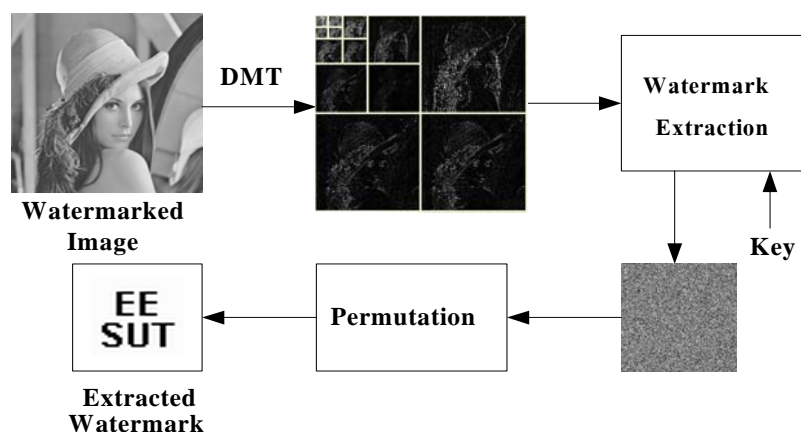


Figure 8.2 Watermark extracting process.

8.2.2.1 Watermark embedding algorithm

The image to be watermarked is first decomposed using DMT into two levels with the DGHM multiwavelet filter. To increase security, the watermark is permuted into scrambled data before embedding. Next, we generate two-dimensional CDMA watermark from permuted watermark and pseudo-random noise pattern with the secret key and then embed watermark directly in the coefficients of

the selected middle bands which are HL_1, LH_1, HL_2 and LH_2 . The selected DMT coefficients are modulated in the following way:

$$I_W(u, v) = \begin{cases} I(u, v) + \alpha \cdot W(u, v), & u, v \in HL_1, LH_1, HL_2, LH_2 \\ I(u, v), & u, v \in LL_2, HH_1, HH_2 \end{cases} \quad (8-1)$$

where $I(u, v)$ is the DMT coefficient from selected subbands, $I_W(u, v)$ is coefficient of watermarked image, $W(u, v)$ and α denote CDMA watermark and the watermark strength, respectively. Finally, we pass the modified DMT coefficients through the inverse DMT to obtain the watermarked image. The watermark embedding algorithm is shown in Figure 8.3.

8.2.2.2 Watermark extracting algorithm

The extraction process is the inverse procedure of the watermark insertion process. We first compute the multiwavelet coefficients of the suspected image. The permuted watermark bits are extracted by analyzing the coefficients and the correlation of pseudo-random sequence used in CDMA generation. Then, we perform inverse permutation of the permuted watermark to obtain the extracted watermark. This technique does not require the original image in watermark extraction. After extracting the watermark, we used normalized correlation in Equation (7-5) to quantify the correlation between the original watermark and the extracted one. The watermark extracting algorithm is shown in Figure 8.4.

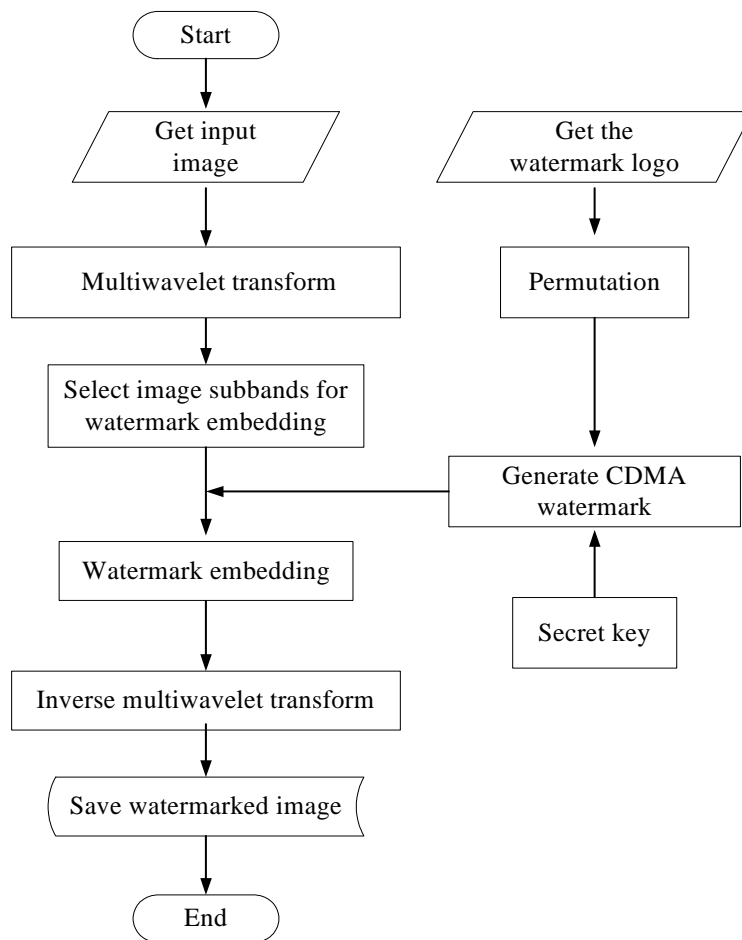


Figure 8.3 Flow chart of the CDMA watermark embedding algorithm.

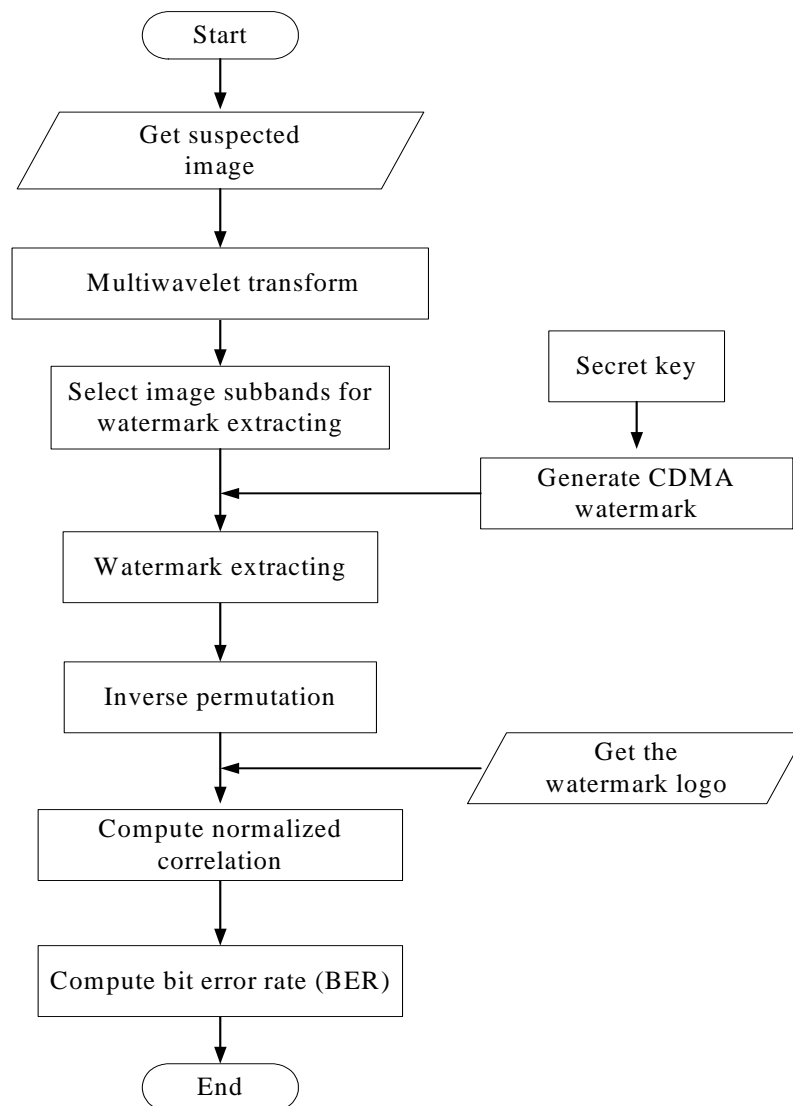


Figure 8.4 Flow chart of the CDMA watermark extracting algorithm.

8.3 Results and Discussions

The experimental results are obtained by using 256 gray-level “Lena” and “Baboon” images of size 512×512 pixels and the binary logo “EE SUT” of size 32×32 pixels as a visually recognizable watermark. Thus, the watermark’s length is 1024. Figures 8.5(a) and 8.5(b) show the original watermark and permuted watermark, respectively.

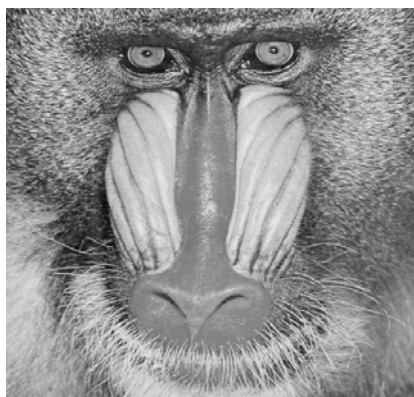
In order to compare robustness between the two techniques in a fair manner, the parameters for each scheme should be adjusted so that watermarked images of approximately the same imperceptibility are produced. In these experiments, the PSNR of watermarked image in each scheme was set to 37 dB. Figure 8.6 to Figure 8.9 show the watermarked version of the Lena and Baboon images from both techniques. It can be seen that most of the watermarked images are not perceptually different from the original ones. In verification phase, the normalized correlation coefficient is compared with a threshold T to determine the existence of a watermark. The threshold T should be chosen to give a relatively small false alarm probability. For the watermark’s length of 1024, we list the false alarm probability for various thresholds in Table 8.1. We choose the threshold $T = 0.4$ which has an associated probability of false alarm less than 1.0221×10^{-38} for a 1024-bit watermark.



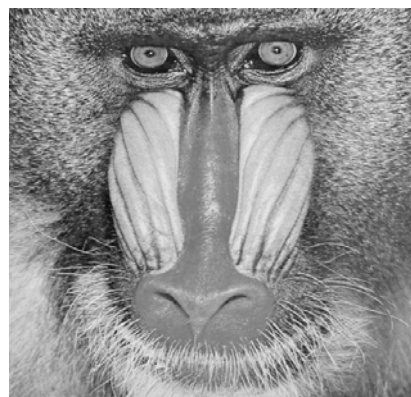
Figure 8.5 (a) Original watermark and (b) permuted watermark.



Figure 8.6 (a) Original "Lena" image and (b) watermarked image from DMT-Tree.



(a)

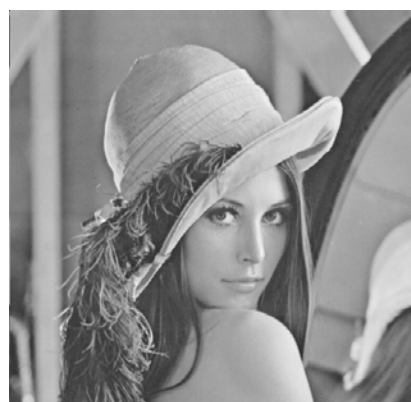


(b)

Figure 8.7 (a) Original “Baboon” image and (b) watermarked image from DMT-Tree.



(a)



(b)

Figure 8.8 (a) Original “Lena” image and (b) watermarked image from DMT-CDMA.

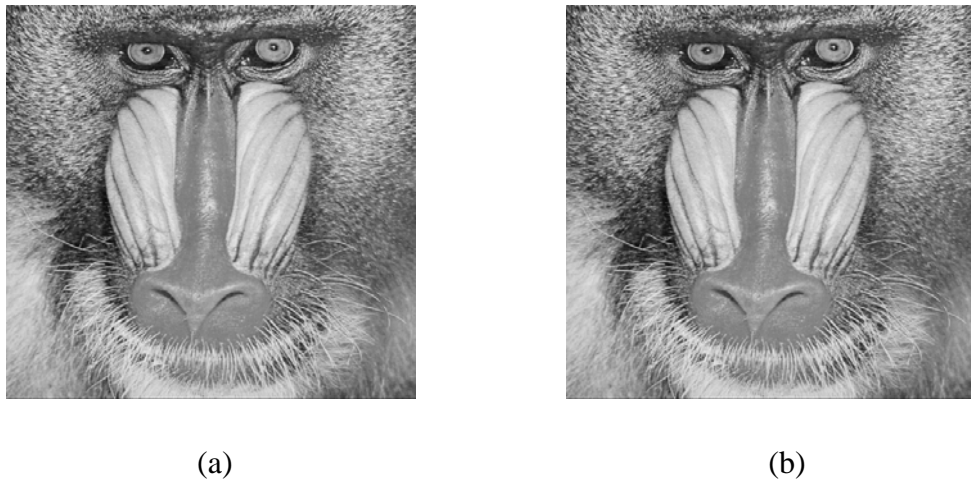


Figure 8.9 (a) Watermarked “Baboon” image from DMT-Tree and (b) watermarked image from DMT-CDMA.

Table 8.1 False alarm probability for different thresholds.

Threshold value	False alarm rate
0.1	6.3825×10^{-4}
0.2	6.4889×10^{-11}
0.3	2.0772×10^{-22}
0.4	1.0221×10^{-38}
0.5	2.8837×10^{-60}
0.6	2.6209×10^{-88}
0.7	8.0526×10^{-123}
0.8	4.0099×10^{-166}
0.9	3.5761×10^{-222}

The watermarked images are attacked using JPEG compression, JPEG2000 compression, and lowpass filtering. Then, we perform the watermark extraction process and then compute the normalized correlation coefficient and the bit error rate (BER). The bit error rate is calculated as the number of incorrectly decoded bits divided by the total number of embedded bits in the watermarked image.

The desirable property of an image watermarking algorithm is the robustness of watermark against lossy image compression. We first attack watermarked image by using JPEG compression. Table 8.2 shows the extracted logo from applying JPEG compression to watermarked images with quality factors 35% to 100%. For multiwavelet tree watermarking technique (DMT-Tree), it can be seen that the extracted logo is still visually recognizable, even for low quality factor as 35%. For watermark robustness against JPEG compression, the detection results (correlation coefficient and BER) are shown in Figures 8.10 and Figure 8.11 for Lena and Baboon images, respectively. We can see that the DMT-Tree method gives more robust watermark than the DWT-CDMA method does.

For watermark robustness against JPEG2000 compression, the detection results are shown in Figures 8.12 and 8.13 for Lena and Baboon image, respectively. We can also see that the DMT-Tree method gives more robust watermark than the DWT-CDMA method does.

Next, the robustness of the watermark is tested by using lowpass filtering. Figures 8.14 and 8.15 show the detection results when the watermarked images are attacked by low-pass filtering using Lena and Baboon image, respectively. The results show that the DMT-Tree method yields more robust watermark than the DMT-CDMA method.

Finally, both watermarking systems are evaluated against a set of attacks from StirMark benchmark (Kutter and Pititcolas, 1999). StirMark is a generic tool developed for simple robustness testing of image watermarking algorithm. It performs a number of manipulations on watermarked images. The StirMark benchmark divides attacks into the following categories: noise-type attacks (median filtering, Gaussian filtering, Frequency Mode Laplacian Removal (FMLR)) and the geometric attacks (rotation with auto-scaling, flip and random geometric distortions). The simulation results using Lena and Baboon images are given in the Table 8.3 and Table 8.4, respectively. The results are similar to other images that were examined. From these tables, we can also see that the watermarking algorithm using multiwavelet tree yields more robust watermark than the one using CDMA technique. Especially, it can survive from well-known StirMark random bending attack, which is a combination of several geometrical attacks followed by other manipulations.

From these experiments, the watermark from the proposed watermarking algorithm is significantly more robust than the one from CDMA watermarking technique. This is due to the predefined structure of multiwavelet tree called “triple tree” of the proposed algorithm. In creation of a triple tree, the multiwavelet-tree is randomly selected using a secret key. The watermark bits spread over all groups of multiwavelet trees. As a result, the watermark is robust against watermark attacks. In addition, the proposed technique utilizes the quantization-based embedding strategy, whereas the CDMA algorithm uses the additive embedding strategy. For CDMA technique, the watermark is easily modified by lossy compression and geometric manipulation.

Table 8.2 Extracted logos from watermarked image after JPEG compression with various quality factors.

JPEG	DMT-Tree		DMT-CDMA	
Quality factor (%)	Lena	Baboon	Lena	Baboon
35				
40				
50				
60				
70				
80				
90				
100				

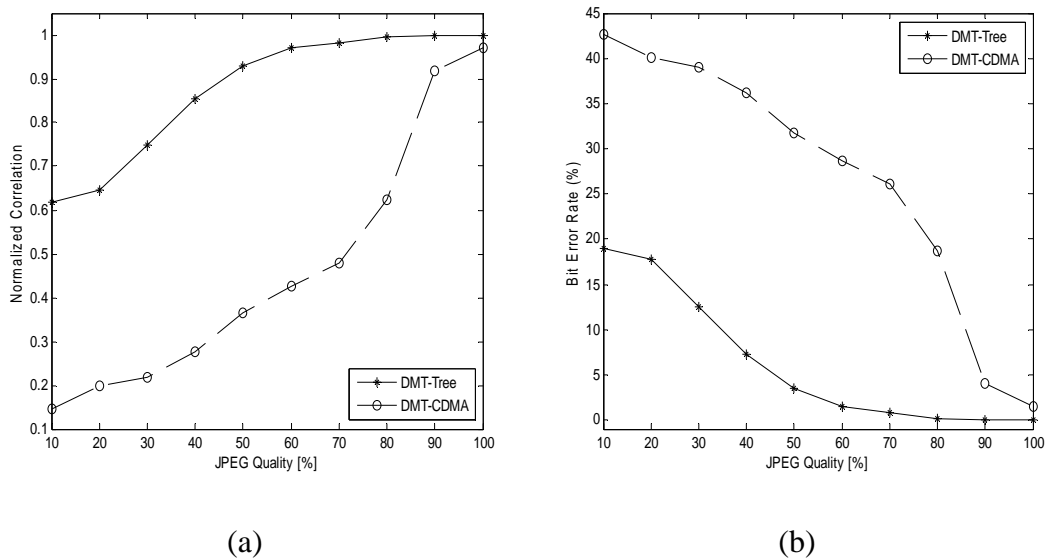


Figure 8.10 Plots of (a) Normalized correlation coefficient and (b) BER versus different JPEG quality factors of JPEG compression using Lena image.

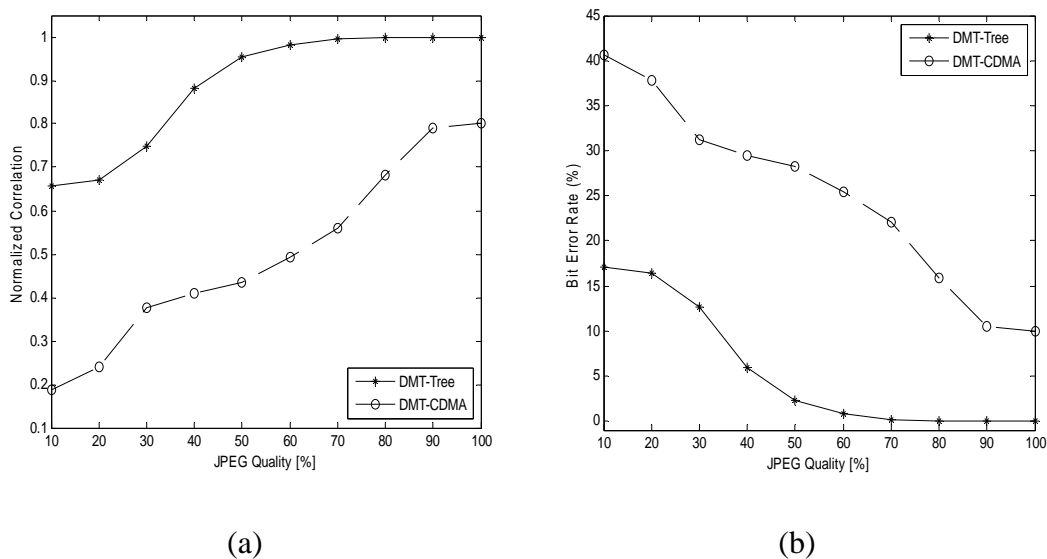


Figure 8.11 Plots of (a) Normalized correlation coefficient and (b) BER versus Different JPEG quality factors of JPEG compression using Baboon image.

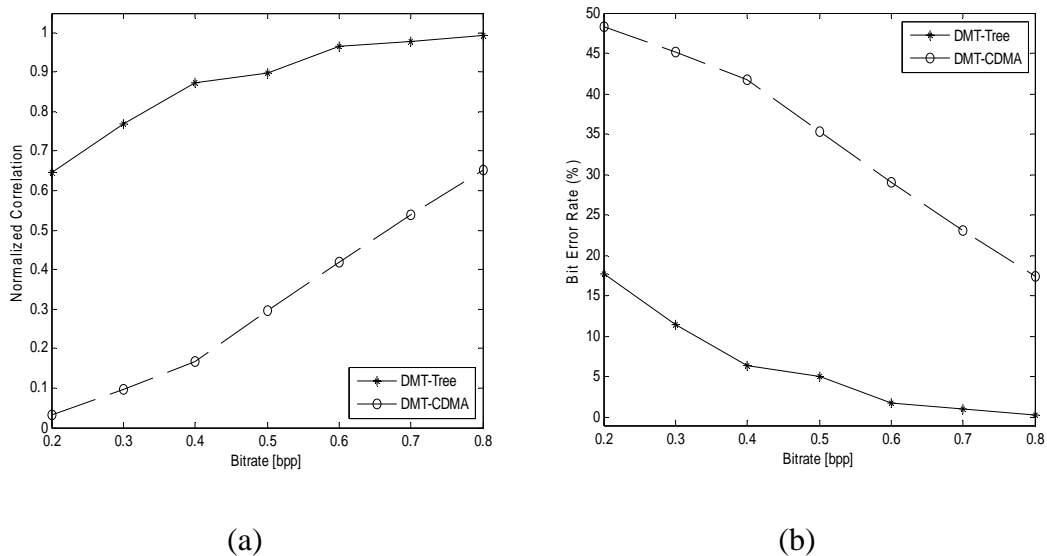


Figure 8.12 Plots of (a) Normalized correlation coefficient and (b) BER versus different bit rates of JPEG2000 compression using Lena image.

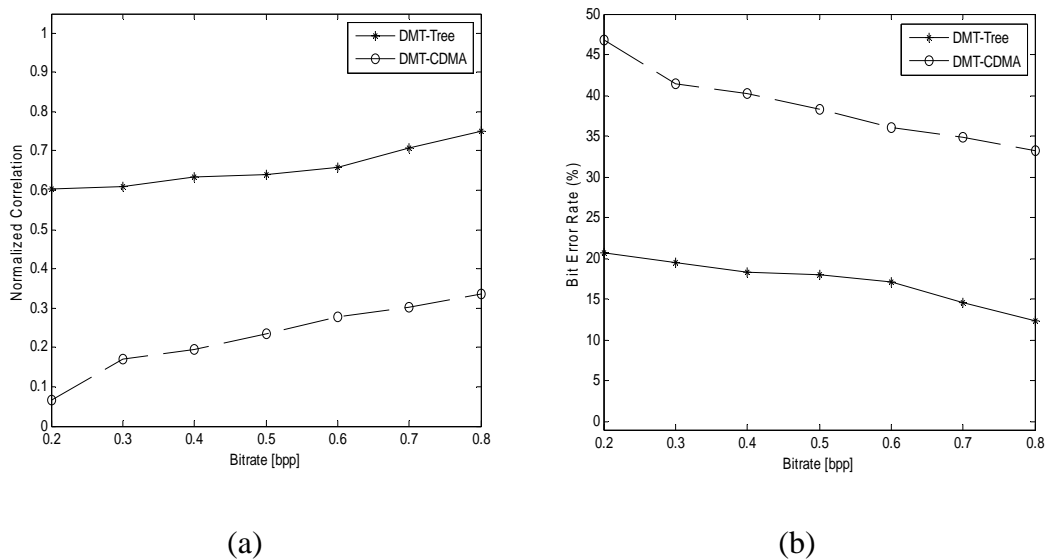


Figure 8.13 Plots of (a) Normalized correlation coefficient and (b) BER versus different bit rates of JPEG2000 compression using Baboon image.

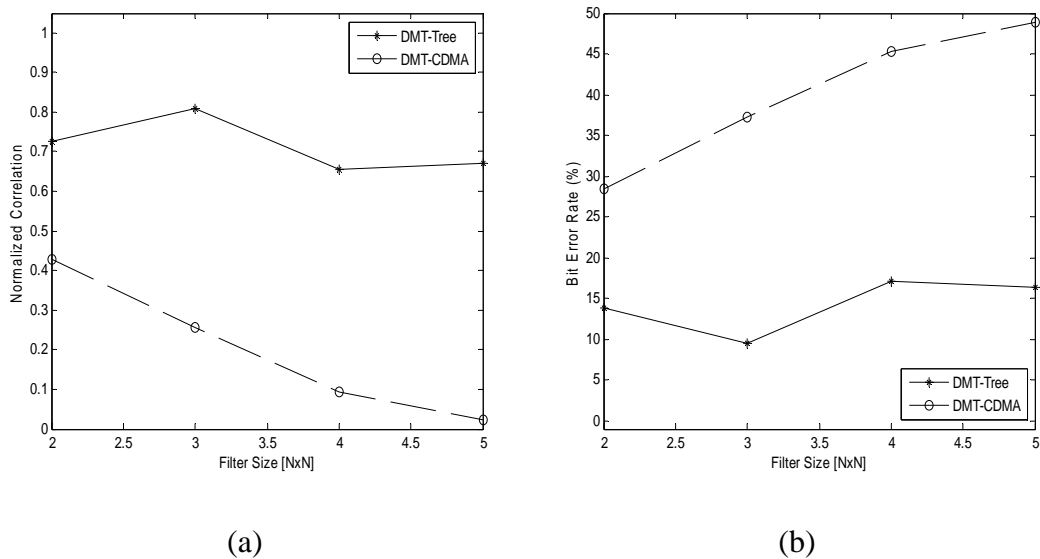


Figure 8.14 Plots of (a) Normalized correlation coefficient and (b) BER versus different filter sizes of lowpass filtering using Lena image.

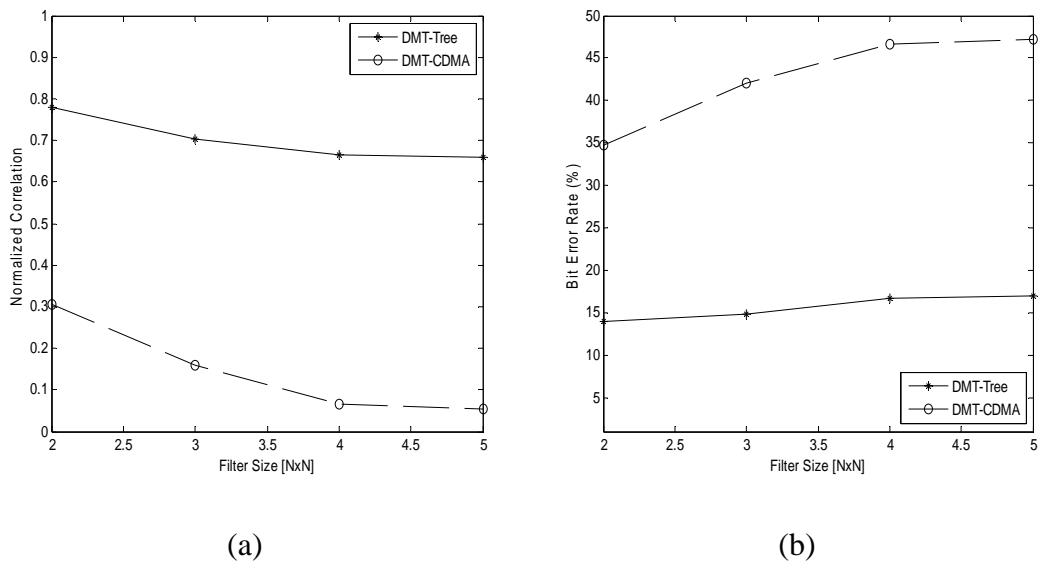


Figure 8.15 Plots of (a) Normalized correlation coefficient and (b) BER versus different filter sizes of lowpass filtering using Baboon image.

Table 8.3 The normalized correlation coefficient and bit error rate from two different multiwavelet-based image watermarking techniques using Lena image.

StirMark Functions	Normalized Correlation		Bit Error Rate	
	Coefficient		(%)	
	DMT-Tree	DMT- CDMA	DMT-Tree	DMT- CDMA
Median_filtering_2x2	0.6934	0.5039	15.33	24.80
Median_filtering_3x3	0.8047	0.7578	9.77	12.11
Median_filtering_4x4	0.6445	0.1387	17.77	43.07
Gaussian_filtering_3x3	0.8613	0.5234	6.93	23.83
FMLR	0.6328	0.4844	18.36	25.78
Flip	0.6211	0.0488	18.95	47.56
StirMark	0.6504	0.0020	17.48	49.90
rotation_scale_-1.0	0.6211	0.0098	18.95	49.51
rotation_scale_-0.5	0.6602	0.0059	16.99	49.71
rotation_scale_0.5	0.6543	0.0391	17.29	51.95
rotation_scale_1.0	0.6094	0.0156	19.53	50.78

Table 8.4 The normalized correlation coefficient and bit error rate from two different multiwavelet-based image watermarking techniques using Baboon image.

StirMark Functions	Normalized Correlation		Bit Error Rate	
	Coefficient		(%)	
	DMT-Tree	DMT- CDMA	DMT-Tree	DMT- CDMA
Median_filtering_2x2	0.6523	0.3672	17.38	31.64
Median_filtering_3x3	0.7031	0.6055	14.84	19.73
Median_filtering_4x4	0.6504	0.0078	17.48	49.61
Gaussian_filtering_3x3	0.7441	0.3340	12.79	33.30
FMLR	0.7422	0.6422	12.89	12.89
Flip	0.6523	0.0488	17.38	47.56
StirMark	0.6621	0.0156	16.89	50.78
rotation_scale_-1.0	0.6738	0.0332	16.31	51.66
rotation_scale_-0.5	0.6699	0.0332	16.50	51.66
rotation_scale_0.5	0.6738	0.0391	16.31	51.95
rotation_scale_1.0	0.6621	0.0156	16.89	49.22

8.4 Chapter Summary

This chapter has presented the performance comparison of image watermarking schemes in the multiwavelet transform domain. The first watermarking scheme is based on the concept of multiwavelet-tree and the second is based on the code division multiple access (CDMA) technique. Using the predefined structure of multiwavelet tree called “triple tree” and the quantization-based embedding strategy, the multiwavelet-tree watermarking technique produces more robust watermark than the CDMA technique does against all attacks which were included in this study such as JPEG compression, JPEG2000 compression, lowpass filtering and a series of selected attacks from StirMark benchmark.

CHAPTER IX

MULTIWAVELET TOOLBOX AND MULTIWAVELET-TREE IMAGE WATERMARKING PROGRAM

9.1 Introduction

This chapter presents the details of the multiwavelet toolbox which can be used in researches and developments of signal and image processing under MATLAB environment. The details of this toolbox include hardware and software requirements, toolbox structures, limitations of toolbox, list of functions in toolbox, an M-file example and execution time testing.

This chapter also presents the multiwavelet-tree image watermarking program which is implemented by using the graphical user interface environment in MATLAB. The details of program include basic requirements, program structure and an example of program usage.

This chapter is organized as follows. Section 9.2 introduces the multiwavelet toolbox for MATLAB. In Section 9.3, the details of multiwavelet-tree image watermarking program are given. Finally, the summary of this chapter can be found in Section 9.4.

9.2 Multiwavelet toolbox for MATLAB

Since multiwavelet transform is used in a smaller research community than wavelet transform, MATLAB does not provide a toolbox related to multiwavelet. Thus, in order to give a tool for beginners to study multiwavelet transform, a multiwavelet toolbox has been created. Each command in the toolbox is written so that it is easy to use. However, users should be familiar with MATLAB basic commands, MATLAB M-files, MATLAB variables. Note that the data structures and memory management will depend on each version of MATLAB. The details of this toolbox will be discussed as follows:

9.2.1 Hardware and software requirements

The minimum hardware requirements are as follows:

- 1) 233 MHz Pentium or higher processors (or equivalent)
- 2) 256 MB of RAM
- 3) 1.5 GB of hard disk free space
- 4) VGA monitor
- 5) Keyboard
- 6) Mouse or compatible pointing device.

The software requirement is MATLAB 6.0 or higher.

9.2.2 Toolbox structure

Multiwavelet toolbox structure can be divided into two parts. The first part is related to one-dimensional signal and the other is related to two-dimensional signal. Each part consists of some commands used to perform multiwavelet decomposition and reconstruction. The block diagrams of multiwavelet decomposition and reconstruction are shown in Figure 9.1 and Figure 9.2, respectively.

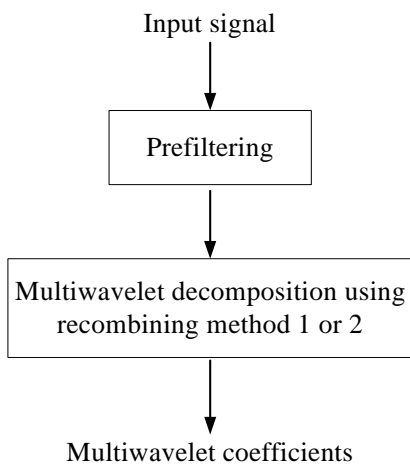


Figure 9.1 Block diagrams of multiwavelet decomposition.

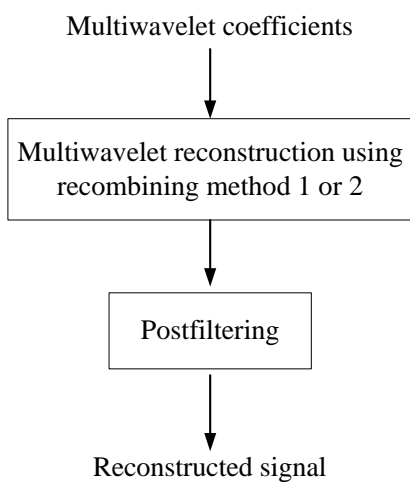


Figure 9.2 Block diagrams of multiwavelet reconstruction.

9.2.3 Limitations of toolbox

The limitations of multiwavelet toolbox are as follows:

- 1) To perform two-dimensional signal decomposition, the input image must be a gray-scale image of size 128×128 , 256×256 or 512×512 pixels only and must be in the format TIF, BMP or JPEG.

2) The multiwavelet decomposition and reconstruction for both one-dimensional signal and two-dimensional signal use the DGHM multiwavelet (Geronimo et al., 1994). The prefiltering process uses the interpolation prefilter or optimal orthogonal prefilter (Attakitmongcol et al., 2001).

9.2.4 List of functions in toolbox

This section provides brief descriptions of all commands which were written in MATLAB functions in the multiwavelet toolbox. The functions are divided into the functions for one-dimensional signal and the functions for two-dimensional signal.

9.2.4.1 Functions for one-dimensional signal

1) Function name: `interPre1D`

Syntax: `pfdata = interPre1D(input)`

Description: Perform prefiltering using interpolation prefilter of one-dimensional signal for the DGHM multiwavelet where “input” is one-dimensional input signal and “pfdata” is the prefiltered signal.

2) Function name: `interPost1D`

Syntax: `rcsignal = interPost1D(recon)`

Description: Perform postfiltering using interpolation prefilter of one-dimensional signal for the DGHM multiwavelet where “recon” is the input for postfiltering process and “rcsignal” is the reconstructed signal.

3) Function name: `optimalPre1D`

Syntax: `pfdata = optimalPre1D(input)`

Description: Perform prefiltering using optimal orthogonal prefilter of one-dimensional signal for the DGHM multiwavelet where “input” is one-dimensional input signal and “pfdata” is the prefiltered signal.

4) Function name: `optimalPost1D`

Syntax: `rcsignal = optimalPost1D(recon)`

Description: Perform postfiltering using optimal orthogonal prefilter of one-dimensional signal for the DGHM multiwavelet where “recon” is the input for postfiltering process and “rcsignal” is the reconstructed signal.

5) Function name: `decom1D`

Syntax: `[low, high] = decom1D(pfddata)`

Description: Perform multiwavelet decomposition of one-dimensional signal where “pfddata” is prefiltered data, “low” is the lowpass output from decomposition process and “high” is the highpass output from decomposition process.

6) Function name: `recon1D`

Syntax: `[recon] = recon1D(low, high)`

Description: Perform multiwavelet reconstruction of one-dimensional signal where “low” represents the lowpass components from decomposition process, “high” is the highpass components from decomposition process and “recon” is the reconstructed signal.

9.2.4.2 Functions for two-dimensional signal

1) Function name: `interPre2D`

Syntax: `Pre_out = interPre2D(I);`

Description: Perform prefiltering using interpolation prefilter of two-dimensional signal for the DGHM multiwavelet where “I” is two-dimensional input signal and “Pre_out” is the prefiltered signal.

2) Function name: `interPost2D`

Syntax: `Post_out = interPost2D(RV_out)`

Description: Perform postfiltering using interpolation prefilter of two-dimensional signal for the DGHM multiwavelet where “RV_out” is the input for the postfiltering process, and “Post_out” is reconstructed signal.

3) Function name: `optimalPre2D`

Syntax: `Pre_out = optimalPre2D(I);`

Description: Perform prefiltering using optimal orthogonal prefilter of two-dimensional signal for the DGHM multiwavelet where “I” is two-dimensional input signal and “Pre_out” is the prefiltered signal.

4) Function name: `optimalPost2D`

Syntax: `Post_out = optimalPost2D(RV_out)`

Description: Perform postfiltering using optimal orthogonal prefilter of two-dimensional signal for the DGHM multiwavelet where “RV_out” is the input for the postfiltering process, and “Post_out” is reconstructed signal.

5) Function name: `dec2Drecombine1`

Syntax: `DEC_out=dec2Drecombine1(Pre_out)`

Description: Perform multiwavelet decomposition of two-dimensional signal with recombining method where “Pre_out” is prefiltered data and “DEC_out” is the output coefficients that have the same size as original signal.

6) Function name: `dec2Drecombine2`

Syntax: `DEC_out=dec2Drecombine2(Pre_out)`

Description: Perform multiwavelet decomposition of two-dimensional signal with recombining method 2 where “Pre_out” is prefiltered

data and “DEC_out” is the output coefficients that have the same size as original signal.

7) Function name: rec2Drecombine1

Syntax: RV_out=rec2Drecombine1(DEC_out)

Description: Perform multiwavelet reconstruction of two-dimensional signal where “DEC_out” is the coefficients from decomposition process which uses recombining method 1 and “RV_out” is the reconstructed signal.

8) Function name: rec2Drecombine2

Syntax: RV_out=rec2Drecombine2(DEC_out)

Description: Perform multiwavelet reconstruction of two-dimensional signal where “DEC_out” is the coefficients from decomposition process which uses recombining method 2 and “RV_out” is the reconstructed signal.

9.2.5 M-file example

The following is a M-file example for performing one-level multiwavelet decomposition and reconstruction of Lena image using the multiwavelet toolbox.

```
% Example of one-level decomposition and reconstruction of Lena image
clear all; % Clear MATLAB workspace
I=double(imread('lena.tif')); % Read input image
figure; imshow(I, []); title('Original image');
Pre_out=interPre2D(I); % Preprocessing
figure; imshow(Pre_out, []); title('Prefiltered image');
DEC_out=dec2Drecombine1(Pre_out); % Multiwavelet decomposition
figure; imshow(DEC_out, []); title('1-Level Decomposition');
RV_out=rec2Drecombine1(DEC_out); % Multiwavelet reconstruction
Post_out=interPost2D(RV_out); % Postprocessing
```

```
figure; imshow(Post_out, []); title('Reconstructed image');
```

```
% ----- End of M-file -----
```

These commands are used to perform multiwavelet transform of image into one-level decomposition and reconstruction. The result of the prefiltered image is shown in Figure 9.3. Figure 9.4 shows the result of one-level decomposition of the Lena image using the DGHM multiwavelet and recombining method 1 which contains 4 image subbands. The result of reconstructed image is shown in Figure 9.5.

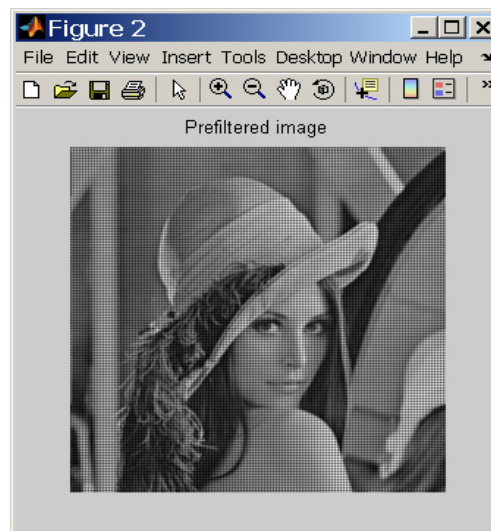


Figure 9.3 Prefiltered image.

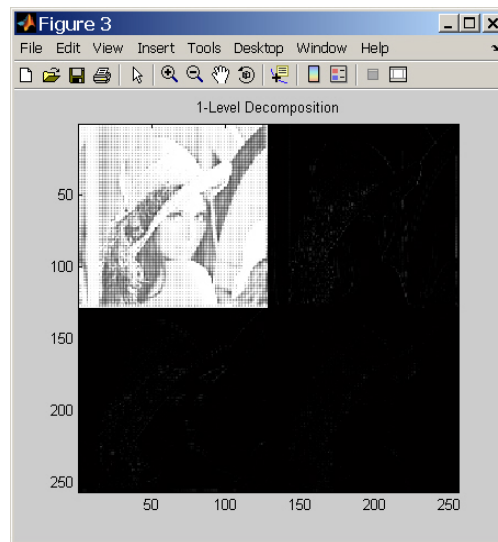


Figure 9.4 Result of one-level decomposition.

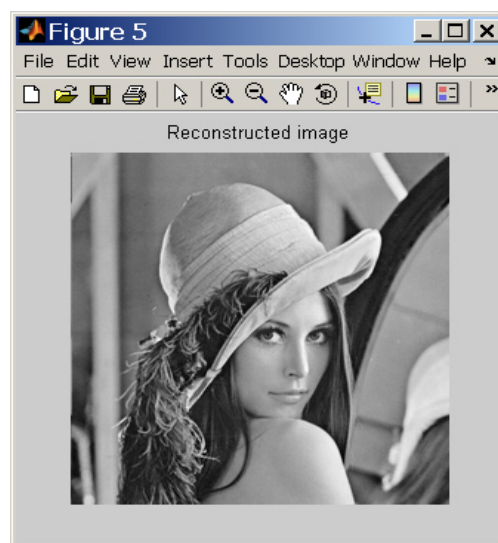


Figure 9.5 Reconstructed image.

9.2.6 Execution time testing

The execution time testing is performed on a personal computer (1.6 GHz Intel Pentium processor, 512 MB RAM, 40 GB hard drive) with Windows XP as the operating system. The testing software includes MATLAB 7.0 and image processing toolbox 4.2.

In testing process, we perform one-level multiwavelet transform of the Lena image which is a gray-scale standard image of size 512×512 pixels. The experiment is performed five times to obtain average execution times. The execution times for multiwavelet decomposition and reconstruction are shown in Table 9.1. The average execution times for multiwavelet decomposition and reconstruction are 3.3469 seconds and 7.4938 seconds, respectively.

Table 9.1 The execution times for multiwavelet decomposition and reconstruction.

	Decomposition time (sec)	Reconstruction time (sec)
1	3.3438	7.5156
2	3.3594	7.5000
3	3.3438	7.4844
4	3.3438	7.5000
5	3.3438	7.4688
Average	3.3469	7.4938

9.3 Multiwavelet-tree image watermarking program

This section explains some of the details of the multiwavelet-tree image watermarking program which provides a user interface incorporating graphical objects such as windows, buttons and text. Selecting or activating these objects usually causes an action to occur. This program is created by using MATLAB GUI functions. The details of the program include basic requirements, program structure and an example of program usage.

9.3.1 Basic requirements

The minimum hardware requirements are as follows:

- 1) 233 MHz Pentium or higher microprocessor (or equivalent)
- 2) 256 MB of RAM
- 3) 1.5 GB of hard disk free space
- 4) VGA monitor
- 5) Keyboard
- 6) Mouse or compatible pointing device.

The software requirement is MATLAB 6.0 or higher. The end users could run this watermarking program without the MATLAB program by installing the MATLAB component runtime (MCR). MCR is a stand-alone set of shared libraries that enable the execution of encrypted M-files created using MATLAB compiler.

9.3.2 Program structure

The structure of the multiwavelet-tree image watermarking program can be divided into 3 parts. The first part is window appearance of the GUI which consists of image, buttons and text. The second part is the watermarking embedding routine and the last part is the watermark extracting routine.

9.3.2.1 Window appearance of the GUI

The program is designed to show the original image and original watermark during the watermark embedding process in the main window. The watermarked image will be saved into the specified directory. During the watermark extracting process, the window shows the suspected image. The result whether the suspected image contains the watermark or not will be displayed in another window. If the suspected image contains the watermark, the extracted watermark will appear in the main window. There are also some buttons in the main window which can be activated by using a mouse or other pointing device. The program is designed for user to enter the embedding and extracting keys. The screenshot of the main window is shown in Figure 9.6.

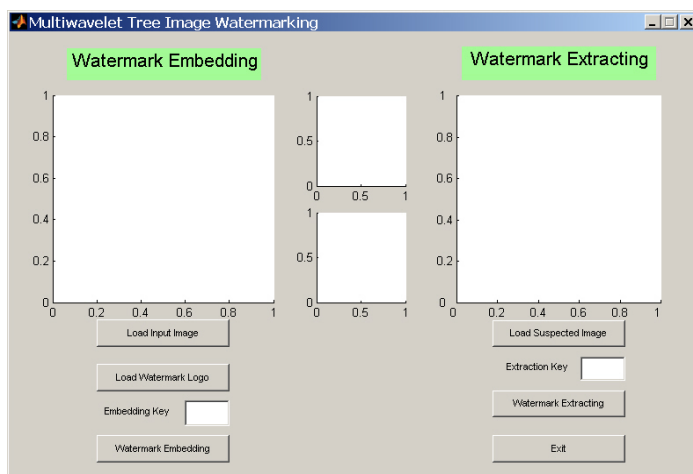


Figure 9.6 Screenshot of watermarking program.

9.3.2.2 Watermark embedding routine

The watermark embedding routine can be described as follows.

- 1) Check the original input image. If the input image is present, go to step 2, otherwise get input image.
- 2) Check the watermark logo. If the watermark logo is present, go to step 3, otherwise get the watermark logo.
- 3) Check the secret key. If the secret key is present, go to step 4, otherwise, get secret key.
- 4) Perform multiwavelet-tree image watermarking by embedding the watermark in the image and display the watermarked image.

The flow chart of this routine can be found in Figure 9.7.

9.3.2.3 Watermark extracting routine

The watermark extracting routine can be describes as follows.

- 1) Check the suspected image. If the suspected image is present, go to step 2, otherwise get suspected image.
- 2) Check the secret key. If the secret key is present, go to step 3, otherwise get secret key.
- 3) Perform watermark extracting to detect the embedded watermark in the suspected image.
- 4) If watermark is present, display the extracted watermark, otherwise display the warning message “The suspected image does not contain our watermark”.
- 5) If watermark is present, compute the bit error rate and normalized correlation.

The flow chart of this routine can be found in Figure 9.8.

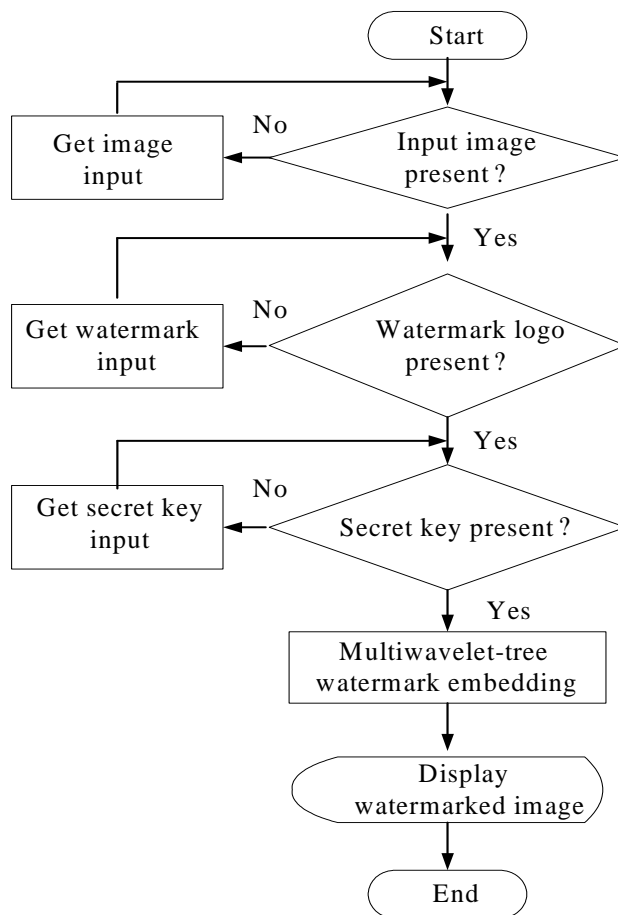


Figure 9.7 Flow chart for watermark embedding routine.

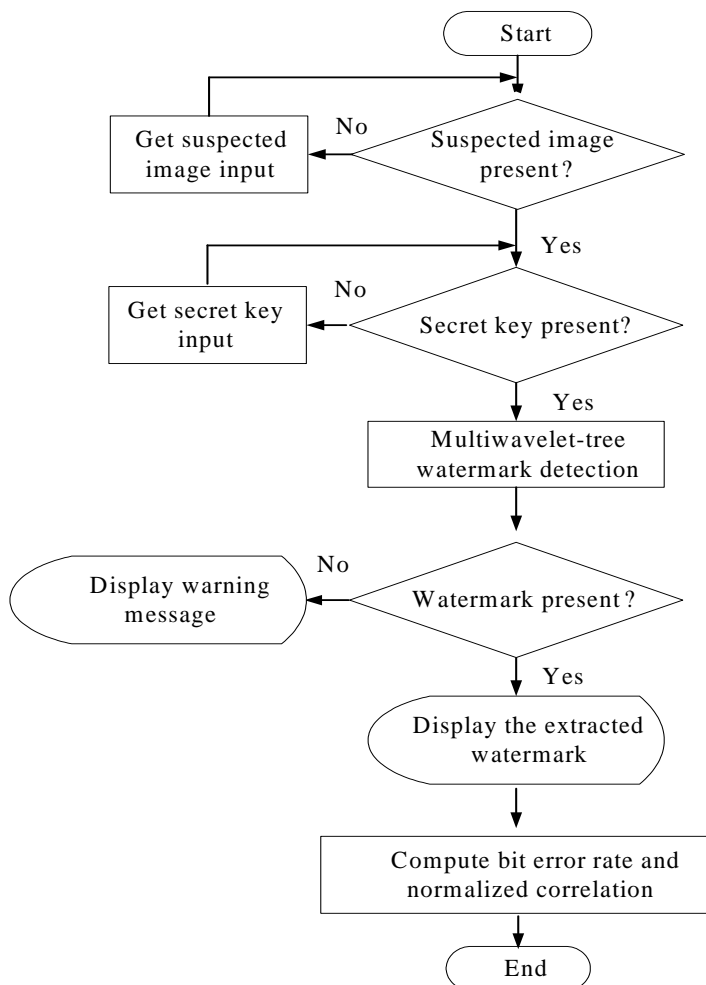


Figure 9.8 Flow chart for watermark extracting routine.

9.3.3 Example of program usage

This example shows the procedures of watermark embedding and watermark extracting using the multiwavelet-tree image watermarking program. The details of both procedures are described as follows:

9.3.3.1 Watermark embedding procedures

- 1) Click the button “Load Input Image” to load input image.
- 2) Click the button “Load Watermark Logo” to load watermark logo.

logo.

3) Input the embedding key at the input text box “Embedding Key”.

4) Perform multiwavelet-tree image watermarking to embed the watermark in the input image by clicking the button “Watermark Embedding”.

This procedure is shown in Figure 9.9. The resulting watermarked image is shown in Figure 9.10.

9.3.3.2 Watermark extracting procedures

1) Click the button “Load Suspected Image” to load suspected image.

2) Input the extracting key at the input box “Extracting Key”.

3) Perform watermark extracting by clicking the button “Watermark Extracting”. This procedure is shown in Figure 9.11. The output result if the suspected image contains the watermark is illustrated in Figure 9.12. If the suspected image does not contain the watermark, a warning message will appear in another window as in Figure 9.13.

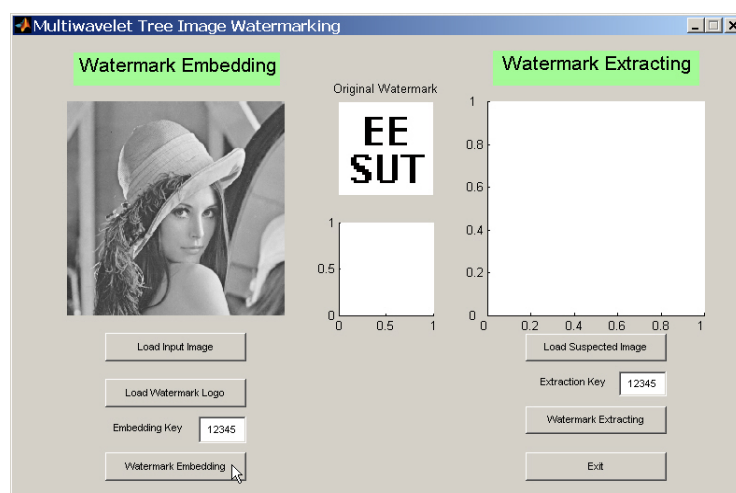


Figure 9.9 Watermark embedding procedure.

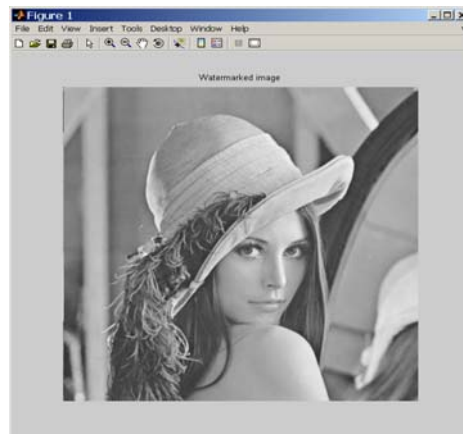


Figure 9.10 Watermarked image.

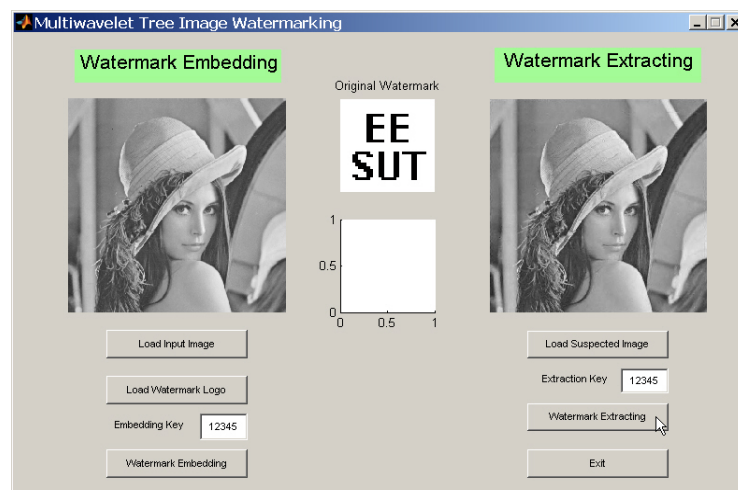


Figure 9.11 Watermark extracting procedure.

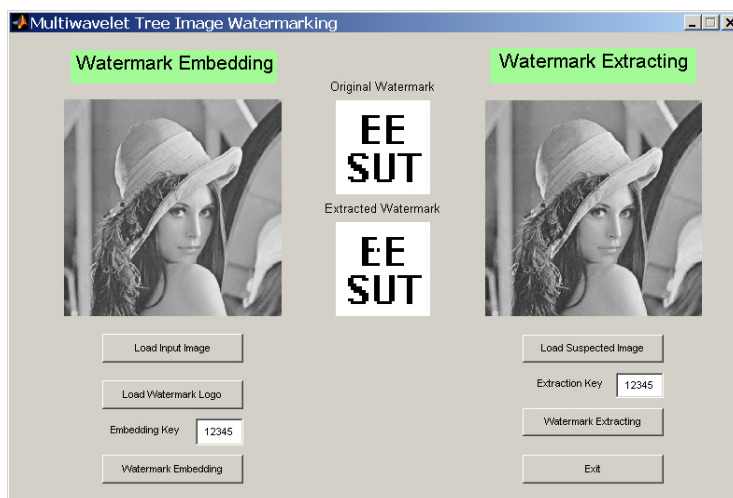


Figure 9.12 Extracted watermark.



Figure 9.13 Warning message if the suspected image does not contain watermark.

9.4 Chapter Summary

This chapter presents the multiwavelet toolbox. The goal of this toolbox is to provide a tool for beginners to study multiwavelet transform in order to use multiwavelet transform in the applications of their interests. This chapter also presents the image watermarking program which is implemented by using the multiwavelet-tree image watermarking algorithm. This program provides a graphical user interface which is easy to use for creating watermarked image or detecting watermark in the suspected image.

CHAPTER X

CONCLUSIONS AND FUTURE STUDIES

10.1 Conclusions

Digital watermarking is one of the most popular approaches considered as a tool for providing the copyright protection of digital multimedia contents. This technique is based on embedding copyright information directly into the digital content in such a way that it always remains present.

The research presented in this thesis is the development of a new digital image watermarking algorithm based on multiwavelet transform for copyright protection application. This thesis consists of five research topics, including the effects of transformation methods on image watermarking, the effects of the recombining processes for the multiwavelet filter bank on image watermarking, performance improvement of image watermarking scheme using genetic algorithms, a novel robust image watermarking technique based on multiwavelet transform and comparative performance of multiwavelet-based image watermarking schemes. The final summary of conclusions are as follows:

10.1.1 Effects of transformation methods on image watermarking

This research topic presents the effects of transformation methods including the discrete cosine, discrete wavelet and discrete multiwavelet transforms on the spread spectrum image watermarking algorithm. Due to the multiresolution representation obtained from using discrete wavelet transform and discrete multiwavelet transform, the algorithms using both transforms yield better

image quality than the one using discrete cosine transform. Moreover, the algorithm using discrete multiwavelet transform gives the most robust watermark under JPEG compression and common signal processing except for lowpass filtering. This is likely due to the fact that for the watermarking in the discrete cosine transform domain, watermark spreads over the set of visually important frequency components.

10.1.2 Effects of the recombining processes for the multiwavelet filter bank on image watermarking

This work investigates the effects of the recombining processes for multiwavelet filter bank on image watermarking. The performance of private and public watermarking schemes with different recombining processes are measured by robustness of the watermarks. The simulation results can clarify the effects of recombining processes for the multiwavelet filter bank on image watermarking in terms of robustness of the watermark. The results show that the watermarking method using the recombining method 1 gives more robust watermark than the one using method 2 does for both private and public watermarking schemes. Therefore, we selected the recombining method 1 for our multiwavelet-based image watermarking scheme.

10.1.3 Performance improvement of image watermarking scheme using genetic algorithms

The contribution of this research topic is the development of a novel approach to improve performance of image watermarking scheme for copyright protection applications. Watermark embedding and watermark detection are performed in the multiwavelet transform domain. In order to achieve the optimum trade-off between perceptual invisibility and robustness of the watermark, we apply the genetic algorithms to search for suitable values of watermarking parameters which are

threshold values and the embedding strength. These parameters are optimally varied to achieve the most suitable for original images with different characteristics. The results show that the performance improvement with respect to the existing algorithms is achieved.

10.1.4 A Novel robust image watermarking technique based on multiwavelet transform

The contribution of this research topic is the design and development of a novel digital image watermarking algorithm in the multiwavelet transform domain for copyright protection application. The new technique is based on the parent-child structure of the transform coefficients called “triple tree”. This technique does not require the original image in the watermark extraction process. The embedded information is 512-bit binary data. Since this information can be not only detectable but also extractable, the watermarking algorithm can be portable to a variety of applications. By the use of Neyman-Pearson criterion, a decision threshold is explicitly derived without referring to the original image. The experimental results show that the proposed watermarking technique is significantly more robust than the Method 1. This is due to the predefined structure of multiwavelet tree called “triple tree” of the proposed algorithm. The watermark bits spread over all groups of multiwavelet trees. As a result, the watermark is robust against watermark attacks. In addition, the proposed technique utilizes the quantization-based embedding strategy. Hence, it gains the watermark robustness to JPEG compression attack.

10.1.5 Comparative performance of multiwavelet-based image watermarking schemes

This research topic presents the performance comparisons of image watermarking schemes in the multiwavelet transform domain. The first watermarking

scheme is based on the concept of multiwavelet-tree, and the second is based on the code division multiple access (CDMA) technique. The embedded information is a binary logo image of size 32×32 pixels which can be extractable without using the original host image. The normalized correlation and bit error rate are used to evaluate the robustness of the watermark. We have demonstrated the robustness of watermarking techniques by using many attacks including JPEG compression, JPEG2000 compression, lowpass filtering and a series of selected attacks from StirMark benchmark. Using the predefined structure of multiwavelet tree called “triple tree” and the quantization-based embedding strategy, the multiwavelet-tree watermarking technique shows superior performance than the code division multiple access technique.

10.2 Future Studies

Since the field of this research topic involves various disciplines such as signal and image processing, digital communications and computer security, there are a number of research directions as extensions of the current work, particularly the ones based on multiwavelet tree. These are the following possible topics for future studies.

1. The development of robust multiwavelet-based image watermarking technique by exploiting the characteristics of the human visual system in watermark embedding process in order to tread off between watermark invisibility and robustness.
2. The development of robust multiwavelet-based image watermarking technique by employing an error control coding in order to decrease the bit error rate of the extracted watermark. The error control coding technique could work well with the proposed watermarking algorithm by encoding the payload prior to the embedding

process. In addition, with the error correction capability of coding technique, the embedded information can be serial numbers, text and other type of digital data. Therefore, the applications of those watermarking algorithms will be broadened.

3. The multiwavelet-tree watermarking algorithm proposed in this dissertation can be extended to digital video watermarking.

REFERENCES

- Attakitmongkol, K., Hardin, D.P., and Wilkes, D.M. (2001). Multiwavelet prefilters II: Optimal orthogonal prefilters. **IEEE Transaction on Image Processing**. 10:1476–1487.
- Brassil, J.T., Low, S., Maxemchuk, N.F., and O’Gorman, L. (1995) Electronic marking and identification techniques to discourage document copying. **IEEE Journal on Selected Areas in Communications**. 13(8): 1495-1504.
- Barni, M., Bartolini, F., Cappellini V., and Piva, A. (1998). A DCT-domain system for robust image watermarking. **Signal Processing**. 66(3): 357-372.
- Barni, M., Bartolini, F., and Checcacci, N. (2005). Watermarking of MPEG-4 video objects. **IEEE Transactions on Multimedia**. Volume 7(1): 23-32.
- Bell, A.E. (1999). The dynamic digital disk. **IEEE Spectrum**. 36(10): 28-35.
- Cheng, Q., and Huang, T.S. (2003) Robust optimum detection of transform domain multiplicative watermarks. **IEEE Transactions on Signal Processing**. 51(4): 906-924.
- Chang, Y.-L., Sun, K.-T, Chen, Y.-H. (2005). ART2-based genetic watermarking. In **Proceeding of the 19th International Conference on Advanced Information Networking and Applications**. (pp.729-734).
- Chu, S.-C., Hsin, Y.-C., Huang, H.-C., Huang, K.-C., and Pan, J.-S. (2005). Multiple description watermarking for lossy network. In **Proceeding of International Symposium on Circuits and Systems**. (pp.3990-3993).

- Copy Protection Technical Working Group. (2006). **Copy Protection Applications** [On-line]. Available: <http://www.cptwg.org/index.html>
- Cox, I.J., and Miller, M.L. (2002). The first 50 years of electronic watermarking. **EURASIP Journal on Applied Signal Processing**. 2002(2): 126-132.
- Cox, I.J., Miller, M.L., and Bloom, J.A. (2001). **Digital Watermarking**. Morgan Kaufmann Publishers.
- Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. **IEEE Transaction on Image Processing**. 6: 1673-1687.
- Dong, P., Brankov J., Galatsanos, N., Yang Y., and Davoine F. (2005). Digital watermarking robust to geometric distortion. **IEEE Transactions on Image Processing**. 14(12): 2140-2150.
- Dugad, R., Ratakonda, K., and Ahuja, N. (1998). A new wavelet-based scheme for watermarking images. In **Proceeding of IEEE International Conference on Image Processing**. (pp.419-423).
- Etter, D., and Ingber, J. (2003). **Engineering Problem Solving with C++**, Prentice Hall.
- El-Khamy, S.E., Lotfy, M.A., and Sadek, R.A. (2002). New technique for perceptual wavelet based image watermarking. In **Proceeding of Radio Science Conference (NRSC 2002)**. (pp.336-343).
- Giakoumaki, A., Pavlopoulos, S., Koutsouris, D. (2003). A medical image watermarking scheme based on wavelet transform. In **Proceedings of the 25th Annual International Conference of the IEEE on Engineering in Medicine and Biology Society**. (pp.856-859).

- Geronimo, S.J., Hardin, D.P., and Massopust, P.R. (1994). Fractal functions and wavelet expansions based on several scaling functions. **Journal of Approx. Theory**. 78: 373-401.
- Hartung, F., and Kutter, M. (1999). Multimedia watermarking techniques. In **Proceeding of IEEE**. 87(7): 1079-1107.
- Huang, C.-H., and Wu, J.-L. (2000). A watermark optimization technique based on genetic algorithms. In **Proceeding of SPIE-Visual Communications and Image Processing**. (pp.516-523).
- Huang, C. -H., and Wu, J. -L. (2004). **Using Genetic Algorithms as Watermarking Performance Optimizers**. [On-line]. Available: <http://www.cmlab.csie.ntu.edu.tw/~bh/oldpage/index.html>
- Hippenstiel, R. D. (2002) **Detection theory: applications and digital signal processing**. Boca Raton CRC Press.
- Hsu, C.T., and Wu, J.L. (1999). Hidden digital watermarks in images. **IEEE Transaction on Image Processing**. 8: 58-68.
- Holland J.H. (1975). **Adaptation in Natural and Artificial Systems**. Ann Arbor: The University of Michigan Press.
- Hsu, C.-T., and Wu, J.-L. (2000). Image watermarking by wavelet decomposition. In **Proceeding of Academy of Information and Management Sciences**. (pp.22-27). USA: Hawaii
- Inoue, H., Mizayaki, A., and Katsura, T. (1999). An image watermarking method based on the wavelet transform. In **Proceeding of IEEE International Conference on Image Processing**. (pp.296-300).

- Joint Photographic Expert Groups. (2006). **JPEG2000 Our New Standard** [On-line]
Available: <http://www.jpeg.org/jpeg2000/index.html>
- Joshi, R.L., Jafarkhani, H., Kasner, J.H., Fischer, T.R., Farvardin, N., Marcellin, M.W., and Bamberger, R.H. (1997) Comparison of different methods of classification in subband coding of images. **IEEE Transactions on Image Processing**. 6(11): 1473-1486.
- Kaldenbach. (2006). **Strategic Digital Music Initiative** [On-line] Available:
<http://www.sdmi.org/index.html>
- Kay, S. M. (1998). **Fundamentals of Statistical Signal Processing Volume II: Detection Theory**. Prentice Hall. New Jersey.
- Kim, J.R., Moon, Y.S. (1999). A robust wavelet-based digital watermarking using level-adaptive thresholding. In **Proceeding of IEEE International Conference on Image Processing**. (pp.226 -230).
- Kumsawat, P., Attakitmongcol, K., and Srikaew, A. (2005). A new approach for optimization in wavelet-based image watermarking by using genetic algorithm. In **Proceeding of the 23rd IASTED International Multi-Conference Artificial Intelligence and Applications**. (pp.328-332).
- Kutter, M., and Pfitzcolas, F.A.P. (1995). A fair benchmark for image watermarking systems. In **Proc. SPIE: Security and Watermarking of Multimedia Content**. (pp.219-239).
- Kundur, D., and Hatzinakos, D. (1998). Digital watermarking using multiresolution wavelet decomposition. In **Proceeding of IEEE International Conference on Acoustics, Speech and Signal Processing**. (pp.2969-2972). USA: Washington.

- Kundur, D., and Karthik, K. (2004). Video fingerprinting and encryption principles for digital rights management. **Proceeding of IEEE**. 92(6): 918-932.
- Kundur, D. (1999). **Multiresolution digital watermarking: Algorithms and implications for multimedia signals**. PhD thesis, University of Toronto, Toronto, Canada.
- Kundur, D., and Karthik, K. (2004). Video fingerprinting and encryption principles for digital rights management. **Proceeding of IEEE**. 92(6): 918-932.
- Kwon, K.-R., and Tewfik, A.H. (2002). Adaptive watermarking using successive subband quantization and perceptual model based on multiwavelet transform. In **Proceeding of SPIE-Security and Watermarking of Multimedia Contents IV**. (pp.334-348).
- Kwon, K.-R., Kang, K.-H., Kwon, S.-G., Moon, K.-S., and Lee, J.-J. (2002). Content adaptive watermarking using a stochastic visual model based on multiwavelet transform. In **Proceeding of International Technical Conference of Circuit/Systems, Computers and Communications**. (pp.1511-1514). Thailand.
- Langelaar, G.C., Setyawan, I., and Lagendijk, R.L. (2000). Watermarking digital image and video data. A state-of-the-art overview. **IEEE Signal Processing Magazine**. 17(5): 20-46.
- Lee, S.-J., and Jung, S.-H. (2001). A survey of watermarking techniques applied to multimedia. In **Proceeding of IEEE International Symposium on Industrial Electronics**. (pp.272-277). Korea.
- Liu, R., and Tan, T. (2000). Content-based watermarking model. In **Proceeding of 15th International Conference on Pattern Recognition (ICPR'2000)**. (pp.238-241).

- Liu, R., and Tan, T. (2000). A new SVD based image watermarking method. In **Proceeding of 4th Asia Conference of Computer Vision (ACCV'2000)**. (pp.63-67). Taiwan.
- Lumini, A., and Maio, D. (2000). A wavelet-based image watermarking scheme. In **Proceeding of Information Technology: Coding and Computing**. (pp.122-127).
- Macq, B., Dittmann, J., and Delp, E.J. (2004). Benchmarking of image watermarking algorithms for digital rights management. **Proceeding of IEEE**. 92(6): 971-984.
- Meerwald, P., and Pereira, S. (2002). Attacks, applications and evaluation of known watermarking algorithms with Checkmark. In **Proceedings of SPIE: Security and Watermarking of Multimedia Contents IV**. (pp.171-175). USA:CA.
- Miller, M.L., and Bloom, J.A. (1999). Computing the probability of false watermark detection. In **Proceeding of 3rd International Workshop on Information Hiding**. (pp.146-158).
- Moving Picture Experts Group. (2005). **MPEG industrial forum** [On-line] Available: <http://www.mpegif.org/index.html>
- Papoulis, A. (1965). **Probability, Random Variables, and Stochastic Processes**, McGraw-Hill. New York.
- Petitcolas, F.A.P., Anderson, R.J., and Kuhn, M.G. (1999). Information hiding - A survey. In **Proceeding of IEEE**. 87(7): 1062-1078.

- Piva, A., Barni, M., Bartolini F., and Cappellini, V. (1997). DCT-based watermark recovering without resorting to the uncorrupted original image. **In Proceeding of IEEE International Conference on Image Processing.** (pp.520-523).
- PodilChuk, C. I., and Zeng, W. (1998). Image adaptive watermarking using visual models. **IEEE Journal on Selected Areas in Communications.** 16: 525-539.
- Proakis, J.G. (1995). **Digital communications.** McGraw-Hill.
- Said, A., and Pearlman, W.A. (1996). A new fast and efficient image codec based on set partitioning in hierarchical trees. **IEEE Transactions on Circuits and Systems for Video Technology.** 6: 243-250.
- Shapiro, J.M. (1993). Embedded image coding using zerotrees of wavelet coefficients. **IEEE Transactions on Signal Processing.** 41(12): 3445-3462.
- Shieh, C.-S., Huang, H.-C., Wang, F. -H., and Pan, J.-S. (2004). Genetic watermarking based on transform domain techniques. **Pattern Recognition.** 37(3): 555-565.
- Weber, A. (2004). **SIPI image database** [On-line] Available: <http://sipi.edu/services/database/Database.html>
- Strela, V., Heller, P.N., Strang, G., Topiwala, P., and Heil, C. (1999). The application of multiwavelet filterbanks to image processing. **IEEE Transaction on Image Processing.** 8: 548-563.
- Tefas, A., Giannoula, A., Nikolaidis, N., Pitas, I. (2005). Enhanced Transform-Domain Correlation-Based Audio Watermarking. **In Proceeding of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '05).** (pp.1049-1052).

- Tirkel, A.Z., Rankin, G. A., Schyndel, R. M., Ho, W. J., Mee, N. R. A., and Osborne, C.F. (1993). Electronic watermark. **In Proceedings of DICTA-93.** (pp.666-672).
- Trichili, H., Boubel, M., Derbel, N., and Kamoun, L. (2002). A new medical image watermarking scheme for a better telediagnosis. **In Proceeding of IEEE International Conference on Systems, Man and Cybernetics.** (pp.556 - 559)
- Song, Y.J., and Tan, T.N. (2000). Comparison of four difference digital watermarking techniques. **In Proceeding of WCCC-ICSP. 2:** 946-950.
- Wang, Z., and Bovik, A.C. (2002). **A universal image quality index.** IEEE Signal Processing Letters. 9(3): 81-84.
- Wang, S.-H., and Lin, Y.-P. (2004). Wavelet tree quantization for copyright protection watermarking. **IEEE Transaction on Image Processing.** 13(6): 154-165.
- Kominek J. (2004). **Waterloo BragZone** [On-line] Available: <http://links.uwaterloo.ca/bragzone.base.html>
- William, P.B., and Joan M.L. (1993). **JPEG still image data compression standard.** Van Nostrand Reinhold. USA: New York.
- Wu, M., Trappe, W., Wang, Z.J., and Liu, K.J.R. (2004). Collusion-resistant fingerprinting for multimedia. **IEEE Signal Processing Magazine.** 21(2): 15-27.
- Xia, X. -G., Boncelet, C., and Arce, G. (1997). A multiresolution watermark for digital images. **In Proceeding of IEEE International Conference on Image Processing.** (pp.26-29).

- Yang, S. H. (2003). Wavelet filter evaluation for image watermarking. In **Proceeding of IEEE International Conference on Acoustics, Speech and Signal Processing**. (pp.525-528).
- Zafeiriou, S.; Tefas, A.; Pitas, I. (2005). Blind robust watermarking schemes for copyright protection of 3D mesh objects. **IEEE Transactions on Visualization and Computer Graphics**. 11(5): 596-607.
- Zeng, W., and Liu, B. (1999). A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images. **IEEE Transaction on Image Processing**. 8:1534-1548.
- Zeng, W., and Liu, B. (1999). A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images. **IEEE Transaction on Image Processing**. 8:1534-1548.
- Zeng, W., Lei S., (1999). Digital watermarking in a perceptually normalized domain. In **Proceeding of the 33rd International Conference on Signals, Systems, and Computers**. (pp.1518-1522).
- Zhang, X. -D., Lo, K. -T., Feng, J., and Wang, D. (2000). A robust image watermarking using spatial-frequency feature of wavelet transform. In **Proceeding of 5th Signal Processing (WCCC-ICSP 2000)**. (pp.1100-1105).
- Zhao, Z., and Yu, N.-H. (2002) A Novel watermark embedding algorithm. In **Proceeding of the 1st International Conference on Machine Learning and Cybernetics**. Beijing.

APPENDIX A
MULTIRESOLUTION ANALYSIS

For many years, multi-scale representations and multiresolution analysis have been proven useful in many image processing applications. Wavelet analysis is an example to generate such a representation. Another form of a multi-scale representation and multiresolution analysis are generated by using multiwavelet transform.

In the basic concept of multiresolution analysis, a signal can be viewed as compositions of smooth background and details on top of it. An important notion of multiresolution analysis within the wavelet representation has been introduced by Mallat (1989). Following his work, a scaling function $\phi(t)$ is said to generate a multiresolution analysis if

- The integer translates of $\phi(t)$ form an orthogonal basis of the subspace V_0 .
- Dilates $2^{-j/2}\phi(2^{-j}t - k)$ generate subspace V_j , $j \in \mathbb{Z}$ such that

$$\dots V_2 \subset V_1 \subset V_0 \subset V_{-1} \subset V_{-2} \dots \subset L^2(\mathbb{R}) \quad (\text{A.1})$$

$$\bigcap_{j \in \mathbb{Z}} V_j = \{0\} \quad (\text{A.2})$$

$$\bigcup_{j \in \mathbb{Z}} V_j = L^2(\mathbb{R}) \quad (\text{A.3})$$

- There exists a wavelet $\psi(t)$ such that its integer translates of $\psi(2^{-j}t)$ form an orthogonal basis of the subspace W_j where W_j is the orthogonal complement of

V_j in V_{j-1} , for example:

$$V_{j-1} = V_j \oplus W_j \quad (\text{A.4})$$

The space W_j is called wavelet vector space. It contains the information needed to go from an approximation 2^j to an approximation at resolution 2^{j-1} . Thus, it follows that

$$V_j = V_k \oplus \bigoplus_{i=j+1}^k W_i \quad (\text{A.5})$$

and

$$\bigoplus_j W_j = L^2(\mathbb{R}) \quad (\text{A.6})$$

The expansion of V_j and W_j is illustrated in Figure A.1.

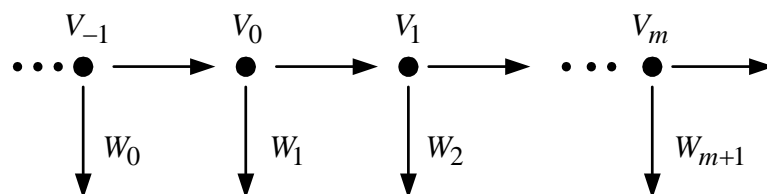


Figure A.1 Space expansion of V_j and W_j .

Since $\phi \in V_0 \subset V_{-1}$, there exists a sequence $h_k \in l^2(Z)$ such that the scaling function satisfies

$$\phi(t) = \sqrt{2} \sum_k h_k \phi(2t - k) \quad (\text{A.7})$$

where h_k are the scaling (lowpass) coefficients, and the $\sqrt{2}$ maintains the norm of the scaling function with the scale of two.

Similarly, since the wavelet $\psi \in W_0 \subset V_{-1}$, there exists a sequence $g_k \in l^2(Z)$ such that

$$\psi(t) = \sqrt{2} \sum_k g_k \phi(2t - k) \quad (\text{A.8})$$

where g_k are the wavelet (highpass) coefficients.

The two-scale relations of the scaling function and wavelet function in (A.7) and (A.8) are called the dilation (refinement) equation and wavelet equation, respectively. It has been shown that the sequence g_k can be obtained from a given sequence h_k via the relation $g_k = (-1)^k h(1-k)$ which implies that an orthogonal wavelet can be derived from an orthogonal scaling function. The wavelet $\psi(t)$ is good at representing the detail and high-frequency parts of a signal. The scaling function $\phi(t)$ is good at representing the smooth and low-frequency parts of the signal.

APPENDIX B
PUBLICATIONS RELATED TO
THE PhD RESEARCH

International Journal Papers

1. P. Kumsawat, K. Attakitmongcol, A. Srikaew and S. Sujitjorn, "Wavelet-Based Image Watermarking Using the Genetic Algorithm," Lecture Notes in Computer Science, Springer-Verlag Heidelberg, Germany, Vol. 3215, pp. 643-649, September, 2004.

2. P. Kumsawat, K. Attakitmongcol and A. Srikaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms," IEEE Transactions on Signal Processing, Vol. 53, pp. 4707-4719, December 2005.

3. P. Kumsawat, K. Attakitmongcol and A. Srikaew, "Comparative Performance of Multiwavelet-Based Image Watermarking Schemes," WSEAS Transactions on Systems, Vol. 5, pp. 1401-1407, May 2006.

International Conference Papers

1. P. Kumsawat, K. Attakitmongcol and A. Srikaew, "The Effects of Transformation Methods in Image Watermarking," Proceeding of the IEEE International Conference on Analog and Digital Techniques in Electrical Engineering (TENCON 2004), November 21-24, 2004, Chiang Mai, Thailand, Vol. 1, pp. 295-298.

2. P. Kumsawat, K. Attakitmongcol and A. Srikaew, "Multiwavelet-Based Image Watermarking Using Genetic Algorithm," Proceeding of the IEEE International Conference on Analog and Digital Techniques in Electrical Engineering (TENCON 2004), November 21-24, 2004, Chiang Mai, Thailand, Vol. pp. 275-278.

3. P. Kumsawat, K. Attakitmongcol and A. Srikaew, “ A New Approach for Optimization in Wavelet-Based Image Watermarking by Using Genetic Algorithm,” Proceeding of the 23rd IASTED International Multi-Conference Artificial Intelligence and Applications (AIA 2005), February 14-16, 2005, Innsbruck, Austria, Vol. 1, pp. 328-332.

4. P. Kumsawat, K. Attakitmongcol and A. Srikaew, “ Multiwavelet Evaluation in Image Watermarking,” Proceeding of the 2005 Electrical Engineering/Electronics, Computer, Telecommunication and Information Technology (ECTI) International Conference, May 12-13, 2005, Pattaya, Thailand, Vol. 2, pp. 546-549.

5. P. Kumsawat, K. Attakitmongcol and A. Srikaew, “Robustness Evaluation of Multiwavelet-Based Image atermarking Techniques,” Proceeding of the 4th WSEAS International Conferences on Application of Electrical Engineering (AEE’06), March 12-14, 2006, Prague, Czech Republic, Vol. 1, pp. 48-53.

Technical Report

1. K. Attakitmongcol, A. Srikaew and P. Kumsawat, “Development of Digital Watermarking Technique using Multiwavelet Transform” The Final Research Report, The National Electronics and Computer Technology Center (NECTEC), Grant NT-B-22-I3-26-47-17, January 2006 (In Thai).

Software Copyright

Title: Digital image watermarking using multiwavelet transform

Applicant Name: Suranaree University of Technology

Inventors: Asst. Prof. Dr. Kitti Attakitmongcol, Asst. Prof. Dr. Arthit
Srikaew and Prayoth Kumsawat

Application Number: 111583

Application Date: October 28, 2005

Recorded by: Department of Intellectual Property, Ministry of Commerce
Thailand.

APPENDIX C

MULTITREE WATERMARK

This appendix illustrates the testing results of the graphic user interface image watermarking program of the multiwavelet-based watermarking using multiwavelet tree. This program is called “MultiTree Watermark”. The MultiTree Watermark is accessible as a stand-alone program for Windows XP. The details of watermarking algorithm can be found in Chapter 7. The screenshot of this program is shown in Figure C.1. The details of test images from digital camera and electron microscope are shown in Table C.1 and Table C.2, respectively. The original images and corresponding watermarked images using the MultiTree Watermark program are displayed in Figure C2 - Figure C7. The results of invisibility and robustness test using images from digital camera and electron microscope are shown in Table C.3 and Table C.4, respectively.

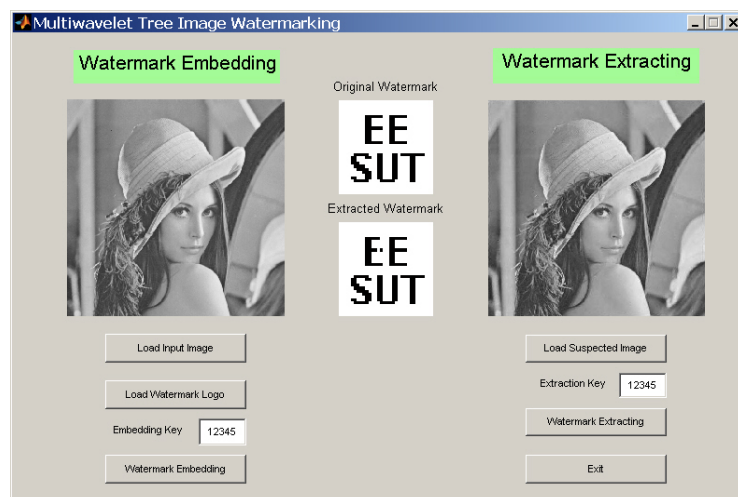


Figure C.1 Screenshot of MultiTree Watermark program.

Table C.1 Images from digital camera (all images are in JPEG file format).

Image name	Size of image	Image name	Size of image
Venice1	480×640	Dear1	2272×1704
Venice2	480×640	Kids1	2272×1704
Panda2	1280×960	Lake	2592×1944
Duck	1280×960	Mountains1	3008×2008
Flowers2	1600×1200	Vanice3	3008×2008
C Garden	1600×1200	Vanice4	3072×2313
Friends1	2048×1536	B1	3072×2304
Friends2	2048×1536	Pine Tree3	3456×2592

Table C.2 Images from electron microscope.

Image name	Size of image	File format
Cell1	512×512	TIF
Cell2	512×512	TIF
Polymer1	2208×1526	BMP
Polymer2	2208×1526	BMP
Bacteria1	2208×1526	BMP
Bacteria2	2208×1526	BMP
Crystal1	2208×1526	BMP
Crystal2	2208×1526	BMP



Original Venice1 image



Watermarked image



Original Venice2 image



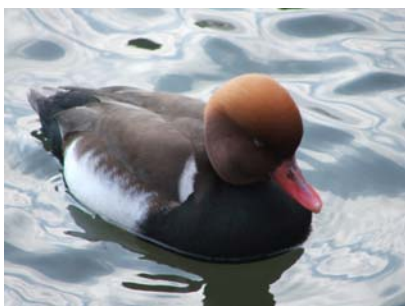
Watermarked image



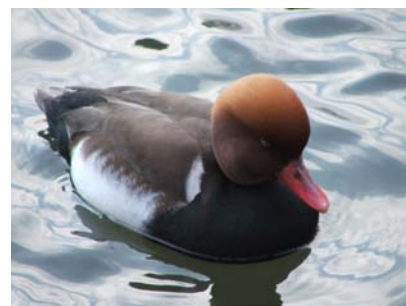
Original Panda2 image



Watermarked image



Original Duck image



Watermarked image

Figure C.2 Original images and watermarked images.



Original Flowers2 image



Watermarked image



Original C Garden image



Watermarked image



Original Friends1 image



Watermarked image



Original Friends2 image



Watermarked image

Figure C.3 Original images and watermarked images.



Original Dear1 image



Watermarked image



Original Kid1 image



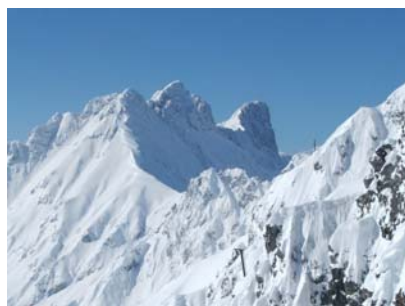
Watermarked image



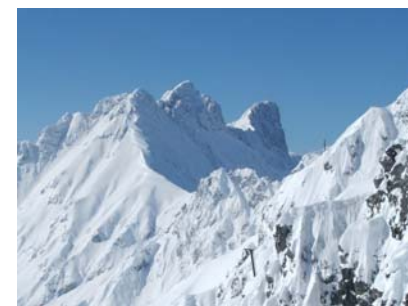
Original Lake image



Watermarked image



Original Mountains image



Watermarked image

Figure C.4 Original images and watermarked images.



Original Venice3 image



Watermarked image



Original Venice4 image



Watermarked image



Original B1 image



Watermarked image

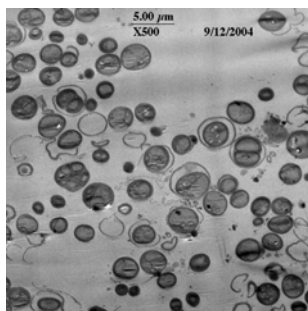


Original Pine tree1 image

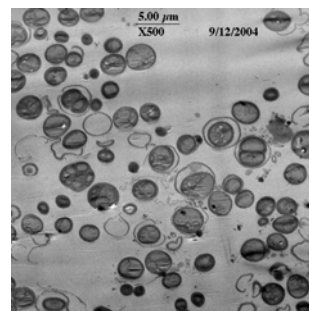


Watermarked image

Figure C.5 Original images and watermarked images.



Original Cell1 image



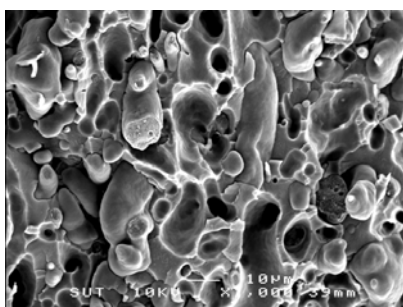
Watermarked image



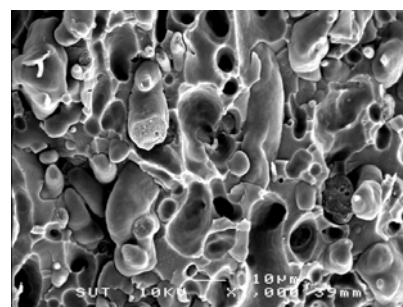
Original Cell2 image



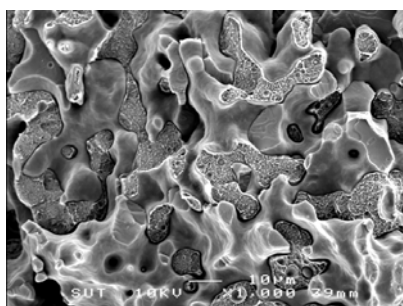
Watermarked image



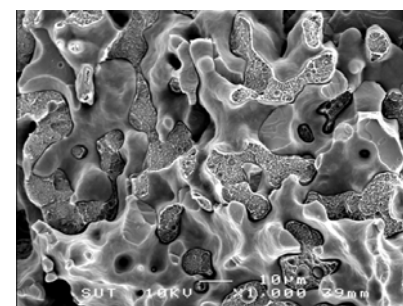
Original Polymer1 image



Watermarked image

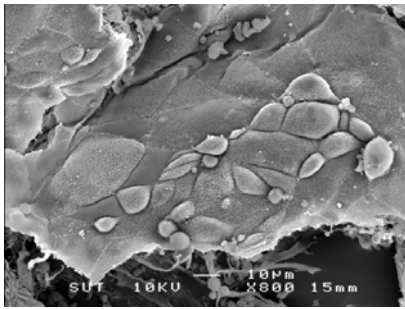


Original Polymer2 image

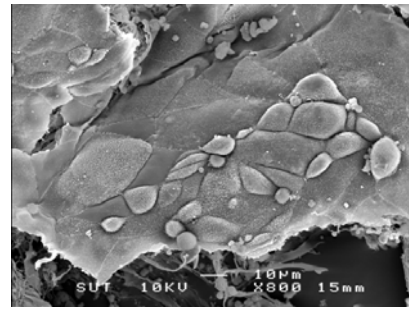


Watermarked image

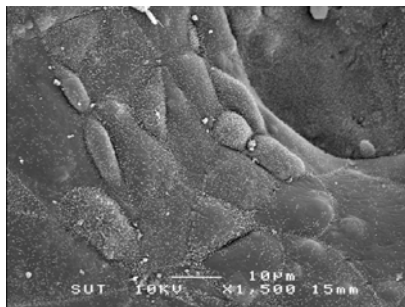
Figure C.6 Original images and watermarked images.



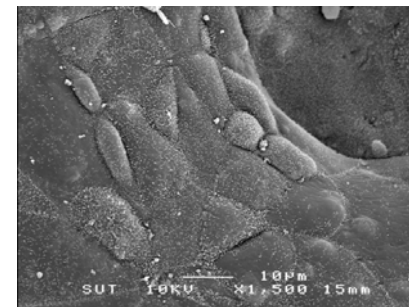
Original Bacteria1 image



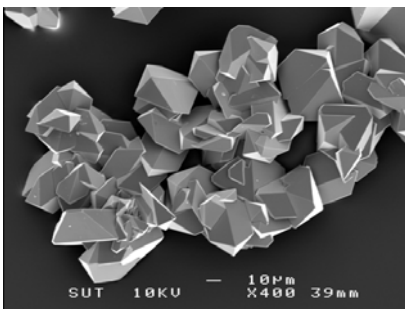
Watermarked image



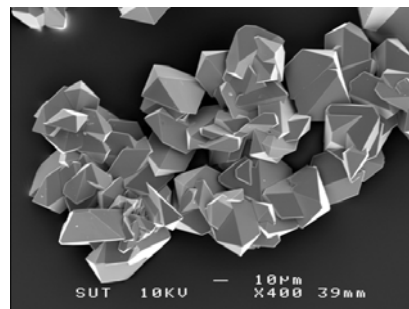
Original Bacteria2 image



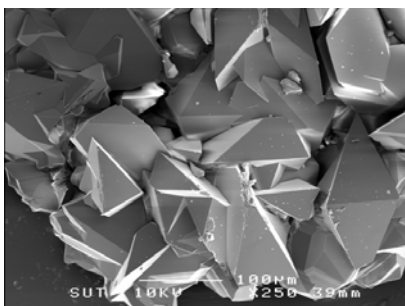
Watermarked image



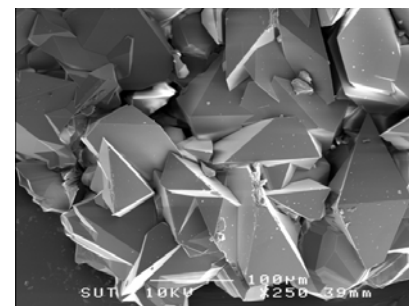
Original Crystal1 image



Watermarked image



Original Crystal2 image



Watermarked image

Figure C.7 Original images and watermarked images.

Table C.3 The results of invisibility and robustness test using images from digital camera.

Image name	PSNR of watermarked image (dB)	Attack by JPEG compression (Quality factor 50%)	
		BER (%)	NC
Venice1	39.20	7.91	0.8418
Venice2	38.44	2.34	0.9531
Panda2	41.85	1.86	0.9629
Duck	45.96	2.93	0.9414
Flowers2	40.10	2.11	0.9570
C Garden	37.12	1.87	0.9623
Friends1	47.70	1.86	0.9629
Friends2	47.15	1.67	0.9611
Dear1	40.38	2.32	0.9551
Kids1	39.01	2.41	0.9523
Lake	51.11	3.52	0.9297
Mountains1	54.17	7.23	0.8555
Vanice3	48.40	5.47	0.8906
Vanice4	46.92	7.81	0.8438
B1	56.84	10.55	0.7891
Pine Tree3	50.23	5.65	0.9012

Table C.4 The results of invisibility and robustness test using images from electron microscope.

Image name	PSNR of watermarked image (dB)	Attack by JPEG compression (Quality factor 50%)	
		BER (%)	NC
Cell1	37.29	4.30	0.9141
Cell2	38.02	5.27	0.8945
Polymer1	49.85	3.13	0.9375
Polymer2	48.87	2.73	0.9453
Bacteria1	46.21	1.86	0.9629
Bacteria2	48.21	1.95	0.9609
Crystal1	55.95	31.05	0.3789
Crystal2	52.99	8.30	0.8340

APPENDIX D

WAVELET TREE WATERMARKING ALGORITHM

This appendix reviews the watermarking algorithm proposed by Wang and Lin (2004). The algorithm is based on wavelet-tree quantization for copyright protection watermarking. The wavelet coefficients were grouped into a predefined structure called supertree. Watermark bits were embedded by quantizing supertree and the resulting difference between quantized and unquantized trees were used for watermark extraction. The watermark embedding and extracting procedures are as follows:

Watermark Embedding Algorithm

1. Generate a seed by mapping a text through a one-way deterministic function.
2. Compute wavelet coefficients of an original image.
3. Group the coefficients and order each group in pseudorandom manner using the seed generated in step 1.
4. Combine every 2 groups to form a supertree.
5. The supertree will be quantized according to the watermark bit to be embedded. Let $\text{round}(x)_i$ denote the rounding of a number x to the i^{th} bitplane. The quantization of $x_n(j)$ with respect to q_n , denoted by $Q[x_n(j)]_{q_n}$, is given by

$$Q[x_n(j)]_{q_n} = \begin{cases} \text{round}(x_n(j))_{a_n} & \text{if } j \leq b_n \\ \text{round}(x_n(j))_{a_n+1} & \text{otherwise} \end{cases} \quad (\text{D.1})$$

where $x_n(j)$ is the j^{th} coefficients of the n^{th} tree, q_n is quantization index and the coordinate of q_n in the array is (a_n, b_n) .

6. Pass the modified wavelet coefficients through the inverse discrete wavelet transform and obtain a watermarked image.

Watermark Extracting Algorithm

The watermark extracting algorithm is as follows:

1. Generate a seed by mapping a text through a one-way deterministic function.
2. Compute wavelet coefficients of an original image.
3. Group the coefficients and order each group in pseudorandom manner

using the seed generated in step 1.

4. Combine every 2 groups to form a supertree.

5. For bit decoding, the watermark decoder examines the corresponding two supertrees T_{2n-1} and T_{2n} . Compute the number of coefficients in T_{2n-1} and T_{2n} . Denote these two numbers by N_{2n-1} and N_{2n} . The embedded bit can now be recovered by comparing N_{2n-1} and N_{2n} as

$$\tilde{w}_n = \begin{cases} -1 & \text{if } N_{2n-1} > N_{2n} \\ 1 & \text{otherwise} \end{cases} \quad (\text{D.2})$$

where \tilde{w}_n is the extracted watermark.

6. Compute normalized correlation coefficient using Equation (7-5).

BIOGRAPHY

Flight Lieutenant Prayoth Kumsawat was born in Maehongson, Thailand, in 1969. He studied in primary school at Khunyoum Wittaya School and in high school at Maesariang Boripat Suksa School. He graduated with the Bachelor Degree of Engineering in Electrical Engineering in 1994 from the Royal Thai Air Force Academy, Bangkok, Thailand. He had worked at the Directorate of Civil Engineering, Royal Thai Air Force for 4 years. He attended Kasetsart University, Bangkok, Thailand and received a Master Degree in Electrical Engineering in 1998. He has been with the School of Telecommunications Engineering, Institute of Engineering, Suranaree University of Technology, Nakhon Ratchasima, Thailand since 1998, and is currently working toward the Ph.D. degree in the School of Electrical Engineering, Institute of Engineering, Suranaree University of Technology. His research interests include multimedia security, digital signal and image processing, and artificial intelligent applications.